

# DEPARTMENT OF HOMELAND SECURITY

## Office of Inspector General

### TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

(REDACTED)

~~SENSITIVE SECURITY INFORMATION~~



~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.~~



Homeland  
Security

September 4, 2008

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002 (Public Law 107-296)* by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

In response to a congressional request from U.S. Representative Bennie Thompson, Chairman of the House Committee on Homeland Security, our report addresses the Transportation Security Administration's (TSA) management of its aviation security activities at the Jackson-Evers International Airport in Mississippi. We also addressed the aviation security activities at five other airports as a means of comparison. We based this review on interviews with TSA employees, federal, state, and local law enforcement officers, commercial airline carrier employees, airport authority staff, direct observations, statistical analysis, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner  
Inspector General

# Table of Contents/Abbreviations

Executive Summary .....	1
Background .....	3
Results of Review .....	13
Current Flying Armed Program Processes Create a Vulnerability to Commercial Aviation Security .....	14
Recommendations .....	20
Management Comments and OIG Analysis .....	20
TSA's Layered Approach Regarding Flying Armed Can Be Improved.....	22
.....	22
Recommendations.....	23
Management Comments and OIG Analysis .....	23
TSO Document Verification Training Needs Improvement.....	25
Recommendations.....	27
Management Comments and OIG Analysis .....	28
TSA Should Conduct Tests to Evaluate the LEO Check In Process .....	29
Recommendations.....	29
Management Comments and OIG Analysis .....	29
Inconsistent Applications of Policies Further Complicate the Flying Armed Process.....	30
Recommendations.....	31
Management Comments and OIG Analysis .....	31
Flying Armed Training Needs Improvement and Better Internal Controls .....	31
Recommendations.....	33
Management Comments and OIG Analysis .....	33
Improper Efforts to Influence Covert Testing Results Exist .....	34
Covert Testing Procedures Can Be Further Strengthened .....	41
Recommendations.....	44
Management Comments and OIG Analysis .....	44
TSA Can Improve Its Processes For Reporting Security Incidents.....	44

# Table of Contents/Abbreviations

---

TSA Should Consider Certain Best Practices .....	47
Operation Centers are Useful Resources for Incident Reporting.....	47
Recommendations.....	49
Management Comments and OIG Analysis .....	49
Additional Educational and Outreach Opportunities Should be Provided to TSOs .....	49
Recommendations.....	50
Management Comments and OIG Analysis .....	50
Incident Report Training and Information Should be Provided to TSOs .....	51
Recommendations.....	52
Management Comments and OIG Analysis .....	52

## Appendices

Appendix A: Purpose, Scope, and Methodology .....	53
Appendix B: Management Comments to the Draft Report .....	55
Appendix C: Congressional Request Letter.....	75
Appendix D: Online Posting of Flying Armed Process .....	77
Appendix E: Summary of Federal Law Enforcement Officers By Agency .....	81
Appendix F: TSA Management Comments to OIG-05-52 .....	82
Appendix G: Timeline of Covert Testing at Jackson-Evers International Airport .....	85
Appendix H: NETHUB Congressional Request Letter .....	86
Appendix I: April 28, 2006, NETHUB Email.....	88
Appendix J: Major Contributors to this Report .....	89
Appendix K: Report Distribution.....	90

## Abbreviations

DHS	Department of Homeland Security
JAN	Jackson-Evers International Airport
LEO	Law Enforcement Officer
OIG	Office of Inspector General
TSA	Transportation Security Administration
TSO	Transportation Security Officer



---

*Department of Homeland Security*  
*Office of Inspector General*

## **Executive Summary**

We reviewed the Transportation Security Administration's management of aviation security activities at Jackson-Evers International and other selected airports as requested by United States Representative Bennie Thompson, Chairman of the House Committee on Homeland Security. Specifically, we assessed (1) whether existing processes, which authorize certain individuals to fly while armed, need strengthening; (2) whether Transportation Security Officers received advanced notice of any internal Transportation Security Administration covert testing; and, (3) whether Transportation Security Officers report the discovery of firearms and other dangerous prohibited items as required by Transportation Security Administration policy and directives. At the request of Chairman Thompson, we expanded our review in November 2007 and investigated whether the Transportation Security Administration compromised any covert testing conducted by another federal government entity. Our investigation disclosed that in an April 2006 internal email, the Transportation Security Administration revealed to its Federal Security Directors and others key details about our covert airport security testing program, including our test methodology and the physical description of one of our undercover testers.

The Transportation Security Administration has made progress toward improving its internal covert testing. Increased resources have allowed the administration to adjust its testing methodology, use sophisticated test equipment, and employ trend analysis to ensure greater testing integrity.

However, additional work is necessary. Most notably, the Transportation Security Administration can take steps to improve security activities within commercial aviation by eliminating the vulnerabilities associated with the current flying armed processes, strengthening covert testing procedures, and improving its processes for reporting security incidents.

Given the size and scope of its airport operations, we are not suggesting that these issues are prevalent across the Transportation Security Administration. However, we note some areas of concern that highlight the need for improvement. Therefore, we are making 12 recommendations to improve the

**~~SENSITIVE SECURITY INFORMATION~~**

**TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports**

**Page 1**

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.

Transportation Security Administration's management of aviation security. These recommendations address near- and long-term solutions to deficiencies we observed. The Transportation Security Administration should work to address the near- and long-term recommendations simultaneously to strengthen its overall layered security approach.

In response to our report, the Transportation Security Administration has proposed plans and actions that, once implemented, will reduce a number of the deficiencies we identified. The Transportation Security Administration concurred with nine recommendations, concurred in part with two recommendations, and did not concur with one recommendation, which we have since modified.

## Background

On September 10, 2006, *The Clarion-Ledger*, a local Mississippi newspaper, alleged in the article “*How Safe Are We?*” that the security and integrity of the passenger screening process at the Jackson-Evers International Airport (JAN) was being compromised routinely by Transportation Security Administration (TSA) employees.

Allegations in the article, made by current and former TSA employees at JAN, concerned three areas:

- First, that Transportation Security Officers (TSO) at JAN received advanced warning of covert testing, even though this testing is to assess airport security operations without notice.
- Second, that JAN management disregarded standard operating procedures by not reporting incidents involving dangerous or deadly items discovered at the airport screening checkpoints.
- Finally, that a passenger at JAN was allowed to board a commercial aircraft armed on at least six occasions, even though this individual did not meet relevant flying armed criteria as set forth in the U.S. Code of Federal Regulations.

On September 11, 2006, Representative Bennie Thompson requested that we review the allegations mentioned in *The Clarion-Ledger* article. On September 12, 2006, Representative Thompson also sent a letter notifying TSA’s Assistant Secretary of his request. On October 4, 2006, we referred this matter to TSA’s Office of Inspection for review. On October 6, 2006, Representative Thompson asked that we reconsider our decision, noting that these allegations raised concerns about the integrity of specific processes and protocols across all of TSA. A copy of the October 6, 2006, request letter is in Appendix C. After reviewing the subsequent request, we agreed to conduct a review of the allegations.

During discussions with Chairman Thompson and his staff, we also agreed to broaden the scope of our review and address four questions.

- Did TSOs at JAN receive any advanced notice of internal TSA covert testing being conducted?
- Did TSOs report the discovery of firearms and other dangerous or deadly items as required by TSA policies and directives?

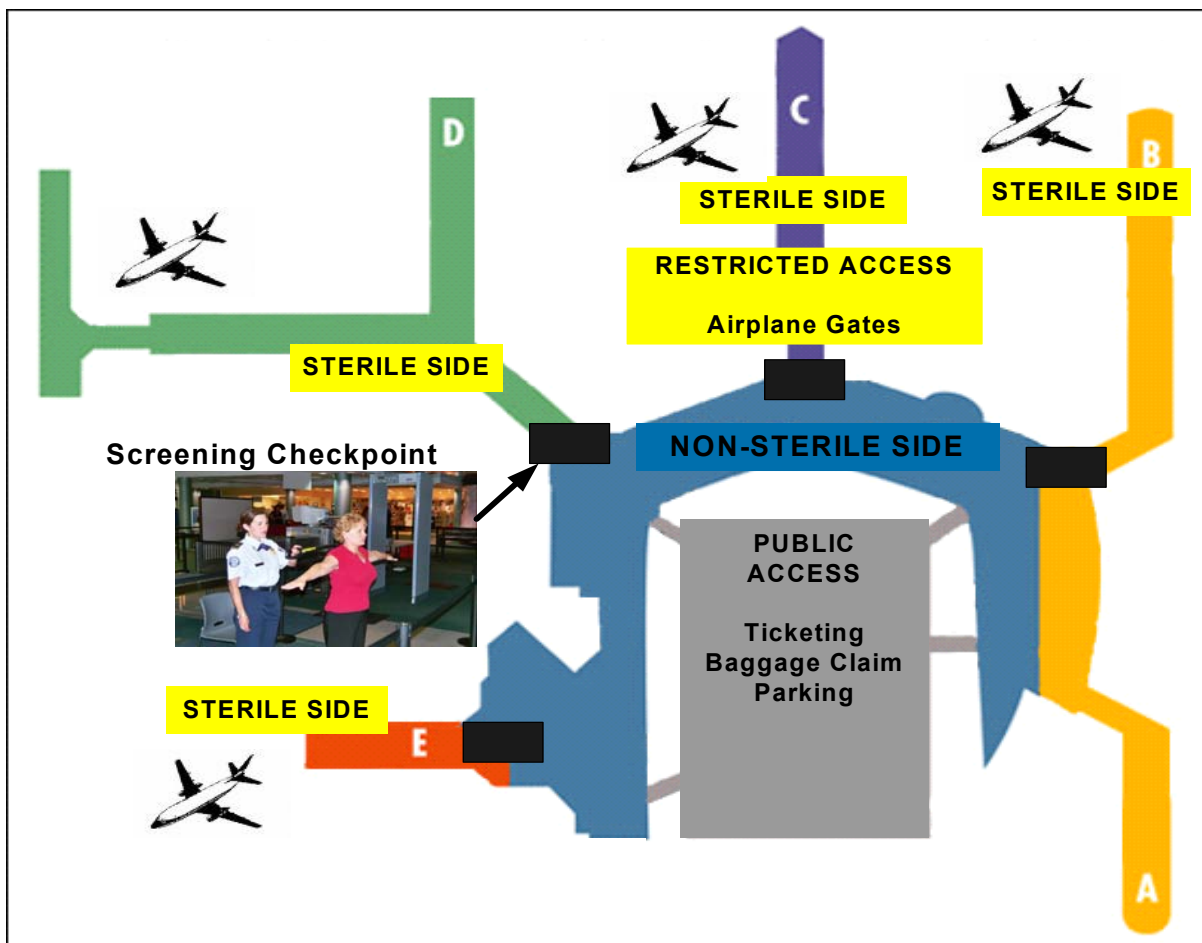
~~SENSITIVE SECURITY INFORMATION~~

**TSA’s Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports**

- Do existing processes, which authorize certain individuals to fly armed, need strengthening? and
- Did TSA compromise any covert testing conducted by another federal government entity?

While each question is distinct, all deal with issues concerning the integrity of an airport's sterile environment – the controlled portion of an airport that is only accessible by screened or authorized individuals. Figure 1 shows the sterile and non-sterile airport environments.

**Figure 1: Sterile and Non-sterile Airport Environment**



In addition to our review, TSA's Office of Inspection conducted two internal reviews pertaining to these allegations. The first review, completed in



September 2006, addressed the issue regarding an individual boarding a commercial aircraft while armed. TSA's review determined the individual had violated the U.S. Code of Federal Regulations. TSA referred the case to the local U.S. Attorney's Office for the Southern District of Mississippi, but the U.S. Attorney declined to prosecute. The second review, completed in November 2006, focused on determining whether JAN's Federal Security Director specifically compromised the integrity of the internal TSA covert tests. The review concluded that the Federal Security Director did not disclose any information concerning TSA covert testing.

Ensuring the integrity of our nation's transportation systems, including the sterile environment of all airports, remains the principal concern of TSA, and any compromises to its security are serious.

## **TSA's Flying Armed Program**

TSA's Office of Law Enforcement/Federal Air Marshal Service and the Office of Security Operations have responsibility for the Law Enforcement Officers Flying Armed Program. Title 49, Section 1544 of the U.S. Code of Federal Regulations, Aircraft Operator Security: Air Carriers and Commercial Operators, provides for the authorization of select law enforcement officers (LEO) to fly commercially while armed, providing they satisfy certain eligibility requirements.

To meet these requirements, an individual must:

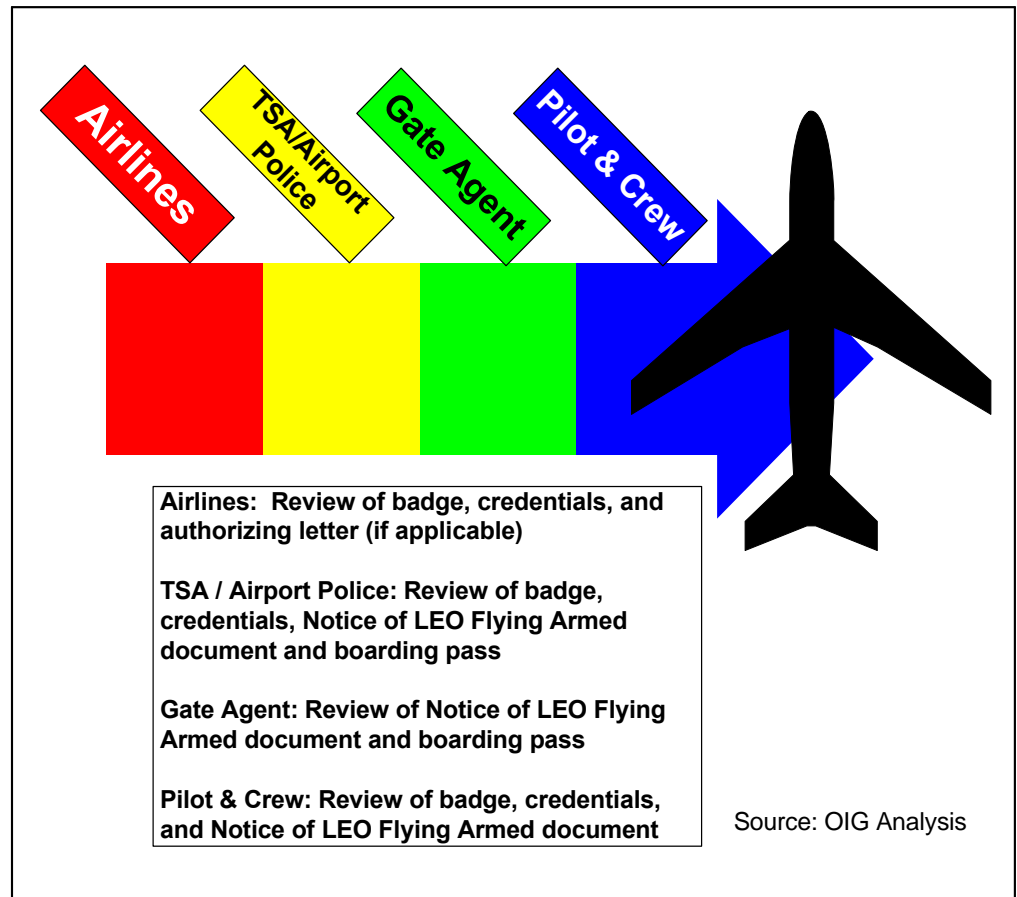
- Be a federal LEO or a full time municipal, county, or state LEO who is a direct employee of a government agency;
- Be sworn and commissioned to enforce criminal statutes or immigration statutes;
- Be authorized by the employing agency to have the weapon in connection with assigned duties;
- Have completed the training program "Law Enforcement Officers Flying Armed;" and
- Comply with all appropriate notification requirements as set forth in the regulations.<sup>1</sup>

---

<sup>1</sup> 49 CFR 1544.219 (a)(1), 49 CFR 1544.219 (a)(2), 49 CFR 1544.219 (a)(3)

Proper compliance with federal regulations requires that each party involved, the LEO, the aircraft operator, and TSA, satisfy specific responsibilities so that a LEO can access the sterile area with their firearm and board the aircraft to meet the LEO's mission requirements. TSA currently relies on a layered security approach to carry out its mission. Figure 2 describes TSA's layered security approach as it relates to the flying armed program.

**Figure 2: TSA's Layered Approach to the Flying Armed Program**



All armed LEOs, upon arrival at an airport, must identify themselves to the aircraft operator's ticketing agent by presenting their credentials and badge. For state, county, or municipal LEOs, they must also present an "original letter of authority, signed by an authorizing official" that confirms the state or local LEO's need to travel armed and the details of their itinerary.<sup>2</sup>

<sup>2</sup> 49 CFR 1544.219(a)(3)(iii)

The ticketing agent is then required to review the officer's badge, credentials, authorizing letter if applicable, and determine whether the officer has completed the official *Law Enforcement Officers Flying Armed* training. The training is required for all federal, state, or local LEOs before they are authorized to fly armed.<sup>3</sup> The training acquaints the officer with the protocols for handling dangerous or prohibited items, prisoner transport, as well as information on avoiding situations that could affect the officer's ability to complete their mission. Once the ticket agent completes this review and is satisfied, the officer must complete a "Notice of LEO Flying Armed" document.

To facilitate an armed LEO's authorized access to a sterile area, TSA has established an alternative process that allows officers to bypass regular passenger screening operations. While this alternative process can vary slightly from airport to airport, depending on infrastructure and the involvement of airport police, [REDACTED], a LEO must present his or her badge, credentials, a second form of government issued photo identification, a commercial airline boarding pass, and the completed "Notice of LEO Flying Armed" document for review.

[REDACTED]

Upon arrival at the departure gate, the aircraft operator's gate agent, among other things, must ensure that the LEO's paperwork is completed and signed, and that the LEO's boarding pass contains the correct name and flight information.<sup>4</sup> The gate agent will notify the flight crew that an armed LEO will be boarding the aircraft.<sup>5</sup> If there are multiple armed LEOs present, the flight crew or gate agent will facilitate the appropriate introductions. The

---

<sup>3</sup> 49 CFR 1544.219(a)(1)(iv)

<sup>4</sup> 49 CFR 1544.219(a)(4)

<sup>5</sup> 49 CFR 1544.219(a)(4)(v)

flight crew also instructs all LEOs not to act in any capacity unless otherwise told to do so by the crew.

Once the gate agent, pilot, and flight crew notifications have been made, and the LEO is seated on board the aircraft, the LEO is required to conceal and maintain immediate physical control of his or her weapon at all times, unless the LEO is in uniform, in which case he or she must keep the weapon on his or her person.<sup>6</sup>

## **TSA's Internal Covert Testing of Passenger and Checked Baggage Screening Procedures**

TSA's Office of Inspection conducts the internal covert testing, or red-teaming, of aviation security operations that are not performed locally at airports. As set forth in TSA's Special Operations Covert Testing handbook and protocols, covert testing, as it relates to airline security, includes the "unannounced, covert tests of security systems, personnel, equipment, and procedures at domestic airports" to determine the effectiveness of "airport passenger security checkpoint screening, checked baggage screening, and airport access controls." These internal covert tests are designed to accurately identify an airport's security posture and to recommend corrective actions, where appropriate, to improve the overall safety and security of domestic airports. These tests are not designed to be performance measures. Rather, they are evaluations of system vulnerabilities that can be used to design countermeasures.

With respect to passenger and baggage screening, TSA's Office of Inspection originally designed its protocols to determine whether prohibited items, such as knives, firearms, or improvised explosive devices, could penetrate security. Should a TSO find a test item, that test is a pass. However, should a test item make its way through security, that test is a fail. The Office of Inspection's team must then determine whether the failure was attributable to an employee, the equipment, a process, or a deficiency related to TSA's standard operating procedures. Should a TSO fail a covert test, the TSO is required to undergo remedial training before performing that particular screening function again.

---

<sup>6</sup> 49 CFR 1544.219(d)

Before the initiation of an internal covert test, TSA's Office of Inspection protocols require advanced notification to the airport police, as well as the airport's Federal Security Director or the director's designee. The covert team leader reminds the Federal Security Director not to inform any TSA personnel that a test is about to commence. Beginning in November 2002, TSA's Office of Inspection set out to test every federalized airport within an initial three-year period.

During this three-year period, larger Category X and I airports were also to be tested either annually or every other year. Categories II, III, and IV were tested at least once during this initial period. Due to resource constraints such as time, funding, and personnel, the Office of Inspection had to plan and conduct internal covert tests of airports that were in the same geographic location. In some instances, TSA covertly tested airports in the same state within a short timeframe.

**Figure 3: Federalized Airports By Category\***

<b>Airport Category</b>	<b>Number of Enplanements Per Year</b>	<b>Number of Airports</b>
<b>X</b>	<b>≥ 5 million</b>	<b>27</b>
<b>I</b>	<b>5 million – 1.25 million</b>	<b>55</b>
<b>II</b>	<b>1.25 million – 250,000</b>	<b>74</b>
<b>III</b>	<b>≤ 250,000</b>	<b>117</b>
<b>IV</b>	<b>Airport served by aircraft of less than 61 seats</b>	<b>179</b>
<b>Total</b>		<b>452</b>
<b>The number of enplanements represents the total number of passengers boarding aircraft.</b> <b>*As of 2007</b>		
		<b>Source: TSA</b>

In 2005, TSA's Office of Inspection developed a new strategy for conducting internal covert tests that focused on emerging trends, threats, and existing screening vulnerabilities. This new strategy focuses primarily on evaluating the effectiveness of screening operations for improvised explosive devices and artfully concealed prohibited items, which concerns the intentional concealment of a dangerous or deadly item. From May 2002 to July 2007, TSA's Office of Inspection conducted more than 800 internal covert tests at airports.

## **Procedures for the Discovery and Reporting of Dangerous Prohibited Items**

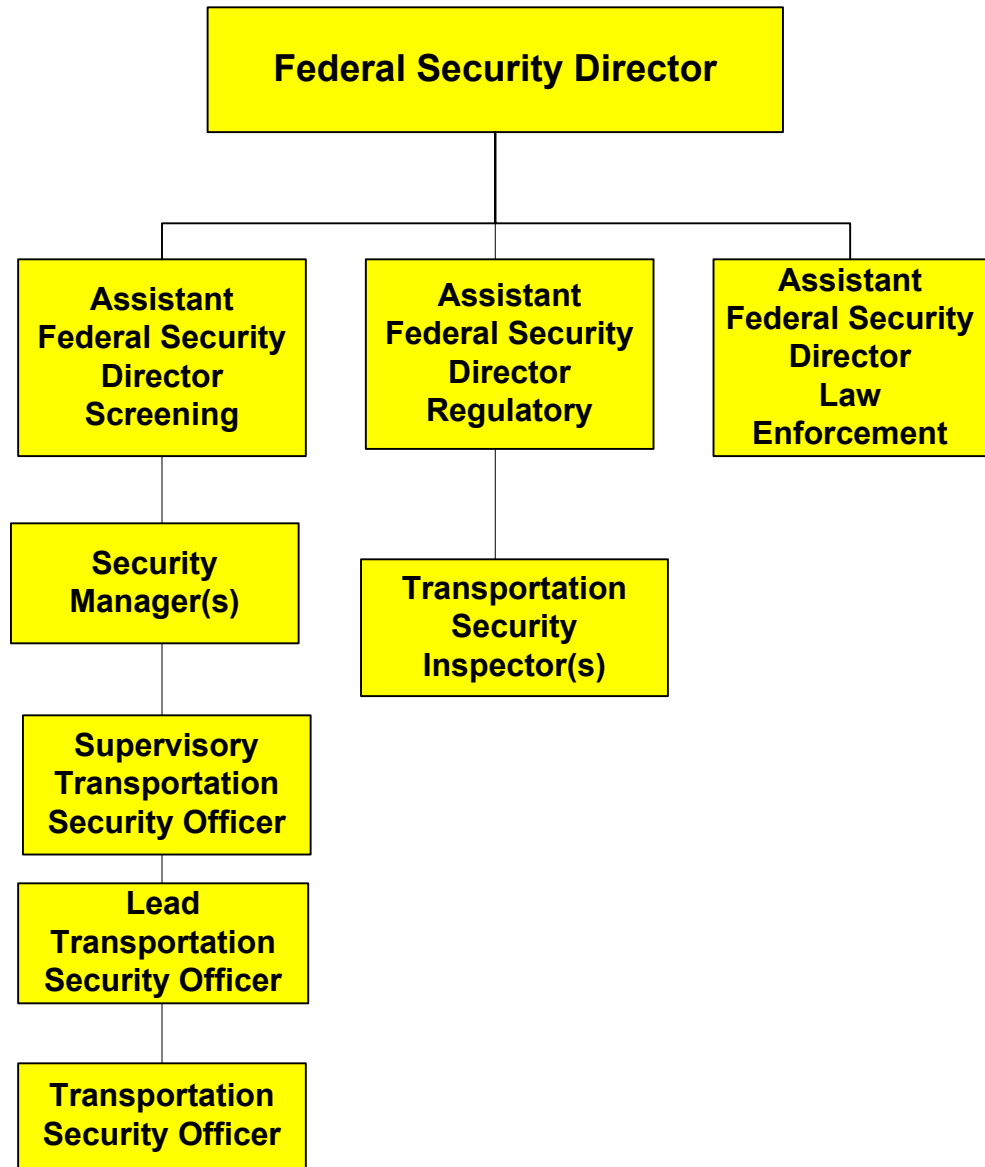
Two TSA Operations Directives, OD-400-18-2B – *Reporting Security Incidents to the Transportation Security Operations Center*, and OD-400-18-1 – *Reporting Security Incidents via the Performance and Results Information System*, govern the discovery and reporting of dangerous or deadly prohibited items.

The first directive, OD-400-18-2B – *Reporting Security Incidents to the Transportation Security Operations Center*, requires that an airport's Federal Security Director, or the director's designee, report the discovery of a dangerous or deadly prohibited item immediately to the Freedom Center, formerly the Transportation Security Operations Center. The Freedom Center is the single point of contact for security-related operations, incidents, or crises within all United States land and air modes of transportation.

The second directive, OD-400-18-1 – *Reporting Security Incidents via the Performance and Results Information System*, states that the Federal Security Director, or the director's designee, is responsible for filing a written report for all incidents involving weapons. These weapons include firearms, bludgeons, explosives, ammunition, disabling or incapacitating items, such as mace, and artfully concealed weapons at their airport or onboard an aircraft that lands at their airport. The Federal Security Director, or designee, has 24 hours to formally report the discovery. This completed report is entered into TSA's Performance and Results Information System, a system designed to track information about security incidents for regulatory and civil enforcement purposes. Annually, TSA enters 70,000 to 80,000 security incident reports in this system.

The discovery and reporting process concerning a prohibited, dangerous, or deadly item can involve several different TSA officials within an airport's chain of command. The traditional TSA Airport Reporting chain of command is illustrated in Figure 4.

**Figure 4: Example of Traditional TSA Airport Reporting Chain of Command**



The three step reporting process (illustrated in figure 5 below) begins when a TSO at a security checkpoint discovers an item, such as a firearm, and notifies the Supervisory TSO assigned to that checkpoint.

The Supervisory TSO will verify that the item is dangerous or deadly, and then alert the airport police. Although the Federal Security Director is responsible for then reporting the incident to the Freedom Center, an Assistant Federal Security Director, a Security Manager, or a TSO may notify the center pursuant to the airport's local protocols. Depending on the nature of the incident, the

Federal Security Director might also contact additional TSA management personnel to keep management apprised of a developing situation.

**Figure 5: Procedures to follow upon discovery of a prohibited, dangerous, or deadly item at a checkpoint:**

<b>STEP 1:</b> Contact the local Airport Police	Performed by either the Supervisory Transportation Security Officer, Lead Transportation Security Officer, or Transportation Security Officer.
<b>STEP 2:</b> Notify the Freedom Center	Responsibility of the Federal Security Director, or their designee, who could be the Assistant Federal Security Director, Security Manager, or Transportation Security Officer.
<b>STEP 3:</b> Contact TSA Headquarters (as needed)	If necessary, the Federal Security Director may contact TSA headquarters to keep headquarters apprised of the situation.

While TSA personnel contact the Freedom Center, the airport police officer would assume custody of the passenger, begin questioning the individual, and then query a number of law enforcement databases for derogatory information about that individual. Should all background checks and questioning produce no negative information, the airport police typically confiscate the item and then release the passenger to fly as scheduled or to rebook his or her flight. However, should derogatory information be revealed, the airport police will detain the individual for additional questioning. Following the conclusion of the event, the attending airport police officer and the Supervisory TSO each prepare incident reports describing the events surrounding the discovery of the prohibited item. The TSO involved prepares a witness statement, if asked, describing his or her role in the discovery of the prohibited item. Should more than one TSO be involved in the event, each TSO would submit a statement. Depending on the reporting guidelines of the airport, a TSO or Transportation Security Inspector would subsequently enter these incident reports into TSA's Performance and Results Information System. The Assistant Federal Security



Director for Regulatory, or another TSA official, would then review, approve, and assign a Transportation Security Inspector to perform a regulatory investigation on the incident.

All notifications to the Freedom Center are documented. However, only incidents deemed significant by TSA management, such as reports on artfully concealed weapons, terminal evacuations, suspicious individuals, or No-Fly list matches, individuals prohibited from boarding a commercial aircraft because of national and aviation security concerns, are included in TSA's daily Executive Summary. The Executive Summary is prepared to brief TSA and other senior Department of Homeland Security (DHS) personnel on the prior day's events. This daily report is descriptive, not analytical in nature.

In addition to TSA efforts, DHS' Office of Operations Coordination and Planning, National Operations Center receives copies of the Executive Summary. TSA has a desk officer at the National Operations Center who identifies emerging issues, and by reviewing TSA's morning brief, the Executive Summary, or other DHS component distributions, funnels this information up through DHS' management reporting structure. The focus of the National Operations Center is real-time department-wide situational awareness. However, National Operations Center officials told us it currently does not conduct any long-term analysis on this information.

## Results of Review

TSA currently employs a risk-based, layered enforcement approach to commercial aviation security, relying on its people, processes, and industry partners to carry out its mission. However, deficiencies exist in the flying armed program, and improvements are needed to TSA's internal covert testing program, as well as the process for reporting security incidents. These deficiencies create vulnerabilities in TSA's layered approach. Although TSA managers acknowledge some of these vulnerabilities, TSA had made limited progress in correcting existing problems, and additional corrective action is necessary. In response to our report, TSA has proposed plans and actions that, once implemented, will reduce a number of the deficiencies we identified.

## **Current Flying Armed Program Processes Create a Vulnerability to Commercial Aviation Security**

Any possible unauthorized access to the sterile environment of an airport compromises the integrity of commercial aviation security and is a serious concern. Those intent on circumventing the screening process are looking to exploit any weakness and might conduct dry runs or tests, and look to take advantage of periods when the system is under tremendous stress, be it during special circumstances, or due to personnel, mechanical, weather-related, or procedural difficulties. Senior TSA officials, as well as federal, state, and local LEOs describe the flying armed program as a weakness in aviation security. This is due in part because:

- The general requirements for flying armed are publicly available, and the process is commonly known to many, including prisoners under the escort of armed LEOs;
- There is no way to independently verify the identity and authenticity of a LEO; and
- TSA's current application of its layered approach toward securing the flying armed program is inconsistent.

Despite having pledged to address issues with this program in the past, TSA management has not made the flying armed program a priority. Instead, TSA continues to rely on the conduct and professionalism of the LEO community, as well as the "sixth sense" of the airport police officers to ensure that only *bona fide* LEOs with a legitimate need are flying armed. However, airport police are not present at every airport and, where present, are not always involved in the process of verifying the flying armed LEO's badge, credentials, boarding pass, and completed "Notice of LEO Flying Armed" document.

Incidents in the past demonstrate the current system is vulnerable to compromise. For example, an incident occurred in March 2007 when police officers at Los Angeles International Airport in California arrested two individuals for impersonating LEOs while attempting to escort a fugitive back to Hawaii. One of the impersonators was armed, and although not compliant with federal regulations, was able to bypass regular checkpoint security screening operations using LEO exit lane procedures, and was prepared to fly armed. Airport police later apprehended the two individuals after the airline

~~SENSITIVE SECURITY INFORMATION~~

**TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports**

gate agent requested that the airport police again review the impersonators' documentation before allowing them to board the aircraft.

### **The Flying Armed Requirements and Processes Are Well-Known**

The general requirements for LEOs flying armed on board commercial aircraft are publicly available in the U.S. Code of Federal Regulations, Chapter XII, Subchapter C, Section 1544.219 – Civil Aviation Security, “Carriage of Accessible Weapons.” Along with these requirements, a quick internet search reveals just how much more information is available on this subject. Some of the information obtained through the quick search is Sensitive Security Information, contained in the *Law Enforcement Officers Flying Armed* training, and should not be available publically. For example, one posting by a metropolitan police department with more than 1,000 sworn officers provides a systematic outline of the entire process, from check-in through boarding. This internet posting also discusses where to go, with whom to speak, and what to do in the event a problem at the airport should arise. Please see Appendix D for more information concerning this internet posting.

In addition, one officer we spoke with expressed concern about how knowledgeable and well-versed prisoners are with the flying armed program, given that these prisoners are escorted through this process while in the company of armed LEOs. This public accessibility to operational knowledge is disconcerting, particularly when the process does not provide for the independent verification of a LEO's identity.

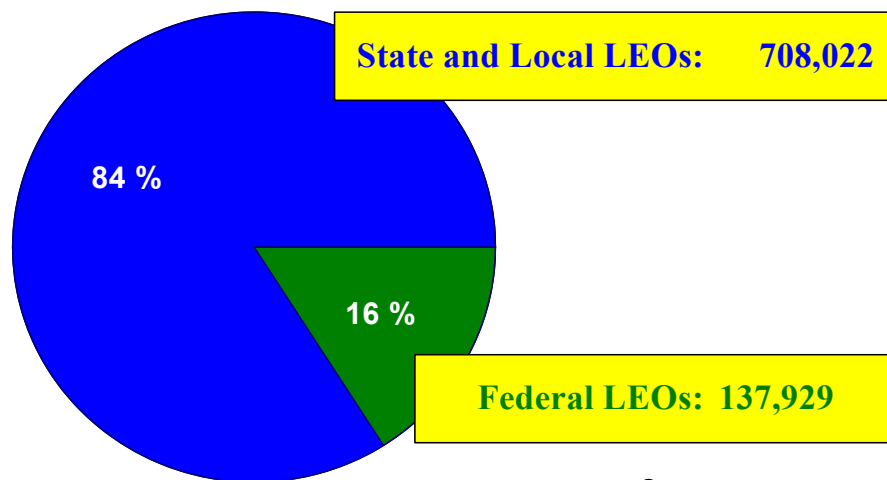
### **There Are No Procedures in Place to Verify the Authenticity of Anyone Claiming to Be a LEO**

[REDACTED]

[REDACTED] there are more than 845,000 federal, state, and local LEOs employed across the United

States.<sup>7</sup> The vast majority of these, roughly 84%, are from the 17,784 state or local departments, while the remaining 16% come from 42 different federal agencies, as shown in Figure 6. Generally, all federal LEOs are authorized to fly armed if they have a mission need to do so. However, only selected state and local LEOs are authorized to fly armed. In our September 2005 report, *Transportation Security Administration's Procedures For Law Enforcement Officers Carrying Weapons On Board Commercial Aircraft*, OIG-05-52, we identified approximately 462,000 annual plane trips with LEOs flying armed, approximately 70% being federal LEOs and 30% being state and local LEOs. In Appendix E, we provide a summary, by organization, of federal LEOs.

**Figure 6: Law Enforcement Community Breakdown**



Source:  
GAO-07-121  
Bureau of Justice Statistics, 2000

Each of the 17,826 departments or agencies issues their own distinctive badge and credential, which typically contain limited or no security features. It has been widely reported in the news media that counterfeit badges are readily available. In 2005, U.S. Immigration and Customs Enforcement officials in New York seized 1,300 counterfeit badges representing 35 different federal, state, and local agencies. In researching this issue, we determined that there are also a number of legal avenues open to anyone looking to obtain an exact

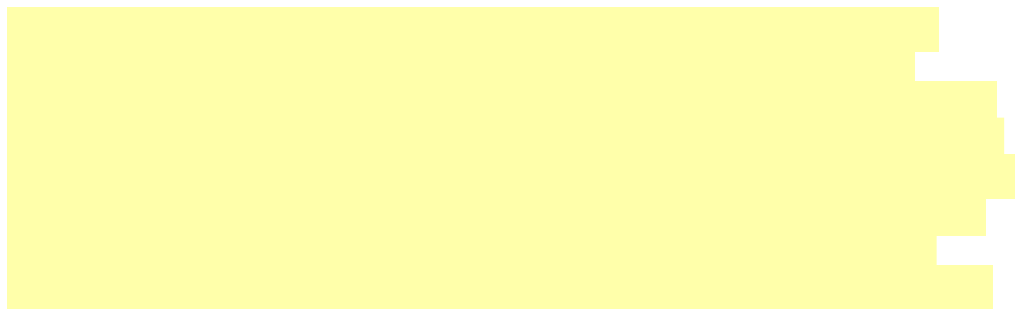
<sup>7</sup> Department of Justice, Bureau of Justice Statistics *Local Police Departments 2000*, and Government Accountability Office's *Federal Law Enforcement: Survey of Federal Civilian Law Enforcement Functions and Authorities*, December 2006, GAO-07-121.

replica of an actual departmental badge. Figure 7 illustrates an example of a replica badge.

Figure 7: Authentic & Replica LEO Badge Comparison



Such a badge, coupled with even a crudely constructed credential and a tri-fold police wallet, and knowledge of TSA's flying armed program procedures, could be enough to get any armed individual on board an aircraft.



<sup>8</sup> 49 CFR 1544.219

<sup>9</sup> 49 CFR 1544.219

### **TSA Efforts to Comprehensively Address Weaknesses Have Not Materialized**

In our September 2005 report, we recommended that TSA take steps to mitigate the vulnerabilities associated with the flying armed program, and TSA concurred.<sup>10</sup> At that time, Congress had recently passed the *Intelligence Reform and Terrorism Prevention Act of 2004*, which directed TSA to establish a LEO credentialing system that incorporates biometric identification technology by April 16, 2005.<sup>11</sup> Biometric technology uses computerized methods to identify a person by their unique physical traits, such as fingerprints or iris recognition scanning.

In its response to our September 2005 report, TSA officials pointed out that Congress did not appropriate funding for the biometric technology, but said it was still working toward mitigating this vulnerability through a number of initiatives. These initiatives included continuing to pilot a biometric identification program at the Ronald Reagan Washington National Airport and the Los Angeles International Airport, which began in July 2004 and ran through November 2005. TSA reported that this pilot program was part of its strategy for working toward implementing a solution for equipping more than 700 security checkpoints throughout the United States with this type of technology.

At that time, TSA officials also said that TSA had developed an online version of the required *Law Enforcement Officers Flying Armed* training, which would provide certificates with a unique identifier to LEOs who completed the training. TSA officials said this would be operational by the end of 2005,

---

<sup>10</sup> *Transportation Security Administration's Procedures For Law Enforcement Officers Carrying Weapons On Board Commercial Aircraft*. Department of Homeland Security Office of Inspector General. OIG-05-52, September 2005. (Sensitive Security Information).

<sup>11</sup> Public Law 108-458, Title IV – Transportation Security, Subtitle B – Aviation Security, Section 4011(a)(6).

and would be used to assist in verifying a LEO if there was a question about their authenticity.

As of May 2008, TSA has not provided our office with any evidence that it has taken steps toward implementing a biometric program since concluding its initial pilot program. As of July 2006, TSA program officials estimated that efforts to initiate a comprehensive biometric identification program would cost approximately \$15 million over an initial three-year period, in addition to some recurring maintenance costs. Despite our repeated requests for additional information, TSA has not provided us with evidence that it developed a final action plan or initiated the appropriate budget requests to implement a biometric solution. In its response to the report, TSA said that fiscal year 2008 and 2009 budgets do not include funding for the development, implementation, or maintenance of a LEO flying armed credentialing requirement. One senior TSA official with knowledge of the program said that senior management has not made this issue a priority.

Regarding an interim online training system, officials from the Federal Air Marshal Service, who assumed control for the flying armed training program in October 2005, said that the online training system was never initiated because of privacy and funding concerns. However, TSA later responded that it determined the Federal Bureau of Investigation's LEO.gov law enforcement portal was the best available vehicle to ensure that the federal, state, and local law enforcement communities have access to the training and best possible information concerning the program.

In lieu of a biometric solution, one TSA management official said that airport management officials often rely on the sixth sense of airport police officers, meaning that police officers are skilled at probing for information in situations that just do not feel right. Putting aside how imperfect this approach is, it can only add some nominal level of enhanced security where airport police are present and involved in the LEO check-in process. In many smaller airports, police officers are not present on site, and even when airport police are present, they are not always involved in the LEO flying armed program to verify a LEO's badge, credentials, boarding pass, and completed Notice of LEO Flying Armed document. Further, one airport police official said that there are too many legitimate credentials for an officer to become familiar with, while another officer said that fraudulent credentials still present one of the biggest "loopholes" in airport security, regardless of who is charged with verification.



## Recommendations

We recommend that the Assistant Secretary for TSA:



**Recommendation #2:** Implement an action plan that establishes funding requirements, necessary resources, and an implementation timeline for a uniform biometric credential that all law enforcement officers will use to gain access to fly armed on commercial airline carriers.

## Management Comments and OIG Analysis

We evaluated TSA's written comments and have made changes to the report where we deemed appropriate. A summary of TSA's written response to the report's recommendations and our analysis of the response follows each recommendation. A copy of TSA's response, in its entirety, is included as Appendix B.

**TSA Response:** TSA concurred in part with Recommendation 1. In its response, TSA noted that they recognize that verifying state and local LEO flying armed authority could be improved. Thus, TSA is working with other components within TSA to provide solutions to improve policies and procedures allowing armed LEOs on domestic flights.

TSA's Office of Law Enforcement / Federal Air Marshal Service recently chartered a working group to develop improved safeguards for the LEO flying armed program. The working group has proposed to use the National Law Enforcement Telecommunication System to send secure messages to TSA when a state or local LEO wants to fly armed. Further, TSA noted that should this solution be adopted, it will provide a more secure and verifiable alternative to the letter of authority.

Federal LEOs are not required to obtain and present a letter of authority from their employing agency. However, in the event that verification is necessary,



TSA's Office of Law Enforcement / Federal Air Marshal Service has developed a 24/7 contact list of federal law enforcement agencies allowing for verification of federal LEOs seeking entry to the sterile area of an airport.

**OIG Analysis:** We consider TSA's proposed actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until TSA provides us with documentation that the proposed use of the National Law Enforcement Telecommunication System has been adopted and implemented by TSA.

**TSA Response:** TSA concurred in part with Recommendation 2. In its response, TSA said they have initiated a process towards a biometric credential. TSA also added that fiscal year 2008 and 2009 budgets do not include funding for the development, implementation, or maintenance of a LEO flying armed credentialing requirement. Thus, the near-term credential verification issues will be resolved through a browser-based electronic LEO logbook, entitled "e-logbook." According to TSA, the e-logbook concept has been developed and initial tests conducted. TSA added that once established, the e-logbook will serve as the platform for later generation biometric based identity verification efforts.

**OIG Analysis:** We consider TSA's proposed actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until we receive documentation that the e-logbook initiative has been implemented within TSA. We also modified the original recommendation where as TSA is not required to report biannually on its progress. We will be monitoring its progress on this recommendation independently.

## **TSA's Layered Approach Regarding Flying Armed Can Be Improved**

We believe, along with some TSA officials, that the implementation of a biometric solution, once initiated, will still take several years to complete. Until that solution is in place, TSA must take additional measures to immediately improve its layered security approach. Specifically, TSA should annually disseminate a letter to all TSA airport security personnel that reiterates the ability of TSA personnel and airport police to perform random searches of law enforcement officer carry-on baggage, ensure greater adherence to operating procedures, improve TSO training, covertly test the exit lane process, and use a standard LEO checkpoint logbook.

[REDACTED]

In our September 2005 report, we recommended that TSA take steps to revise its procedures to ensure that a LEO's carry-on baggage be manually inspected before permitting a LEO access to the sterile area, until TSA could implement a uniform biometric solution.

[REDACTED]

Concerning the underlying issue of LEO verification, TSA officials said the only "workable solution" to this issue would be implementing an effective biometric solution, which would render LEO baggage searches unnecessary. Again, TSA mentioned the online version of the required flying armed training as an interim fix, until TSA could implement a biometric solution. In response, we revised the recommendation we made in the September 2005 report and recommended that TSA inspect a sample of LEO's carry-on baggage.

[REDACTED]

We agree with TSA's assertion that the underlying issue is LEO verification, and that a biometric solution is the only viable way to resolve this issue. However, TSA has made limited progress in implementing such a solution. Until TSA has implemented a LEO credentialing system that incorporates biometric identification technology, disseminating a letter to all TSA airport security personnel that reiterates the ability of TSA personnel and airport police to perform random searches of law enforcement officer carry-on

---

<sup>12</sup> OIG-05-52, September 2005. TSA Management Comments are included as Appendix F.

baggage is prudent and necessary. The inspection provides an added layer of security against the penetration of not just weapons, but improvised explosive devices into the sterile environment of an airport, which, according to TSA's own threat-based analysis, pose a more significant threat to aviation security. While we agree that such searches do create some operational constraints, TSA should find ways to mitigate these constraints until a biometric solution is operational.

## Recommendations

We recommend that the Assistant Secretary for TSA:



## Management Comments and OIG Analysis

**TSA Response:** TSA did not concur with this recommendation. In their response, TSA stated that the recommendation, in its current form, was operationally unfeasible and would not mitigate the vulnerability cited in the report. TSA added that although they share the goal of improving the LEO flying armed process, they cannot endorse a recommendation that would make LEOs less secure while not appreciably improving the screening detection process. TSA also noted that should there be a reasonable belief that an individual seeking sterile area access is not authorized to fly armed, or may be impersonating a LEO, TSA personnel and airport police are required to verify the authority of the individual by agency phone calls, National Crime Information Center checks, additional identification checks, and, if necessary, a complete screening of the individual.

**OIG Analysis:** As presented, we do not consider TSA's comments responsive to the recommendation, which remains unresolved and open. However, in response to TSA's comments we modified the initial recommendation as follows:

**Modified Recommendation #3:** Annually disseminate a letter to all TSA airport security personnel that reiterates the ability of TSA personnel and airport police to perform random searches of law enforcement officer carry-on

baggage. This recommendation would be in place until a uniform biometric credential is operational.

[REDACTED]

[REDACTED]

**Management Must Ensure Greater Adherence to Existing Standard Operating Procedures**

TSA standard operating procedures require that [REDACTED]

[REDACTED]

verification purposes. We spoke with TSOs and Supervisory TSOs at one airport who said they are not asking for any second form of identification. Several security managers we spoke with at the same airport did not realize this was a TSA standard operating procedure requirement. When asked, one Security Manager said that they did not routinely ask for a second form of identification, except when a TSO had a question about a credential.

TSA management must ensure that all TSOs adhere to standard operating procedures, [REDACTED]

[REDACTED]


### **TSO Document Verification Training Needs Improvement**

While ensuring adherence to its standard operating procedures for document verification, TSA also should enhance its document verification training for TSOs. To the extent that TSOs are now performing this check, we have concerns that TSOs do not have an adequate level of training to satisfactorily perform this function. Again, in response to our September 2005 report, TSA said that it would consider intensifying the training it provides TSOs and Supervisory TSOs to further enhance their understanding of fraudulent documents.

However, as of July 2007, TSOs involved in processing LEOs are still only required to complete TSA's Credential Verification training course, available through its On-line Learning Center. We reviewed this course and determined that the subject matter as presented is inadequate for verification purposes, particularly when compared to other available public and private sector training. For instance, other training options consist of comprehensive interactive online training tools, and instructor led courses that incorporate the use of specific identification methods to verify unique security features contained in identity documents.

After raising this concern again, TSA officials said that TSA's Office of Security Operations was conducting a Travel Document Checker pilot program. The term "travel document" refers to the various forms of identification used to enter the sterile area of an airport through the passenger-screening checkpoint including tickets, boarding passes, and government-issued photo identification. The pilot program consists of TSOs manually reviewing documents to determine whether current technology could add to the security posture of an airport, and not hinder the processing or increase the wait times for passengers.

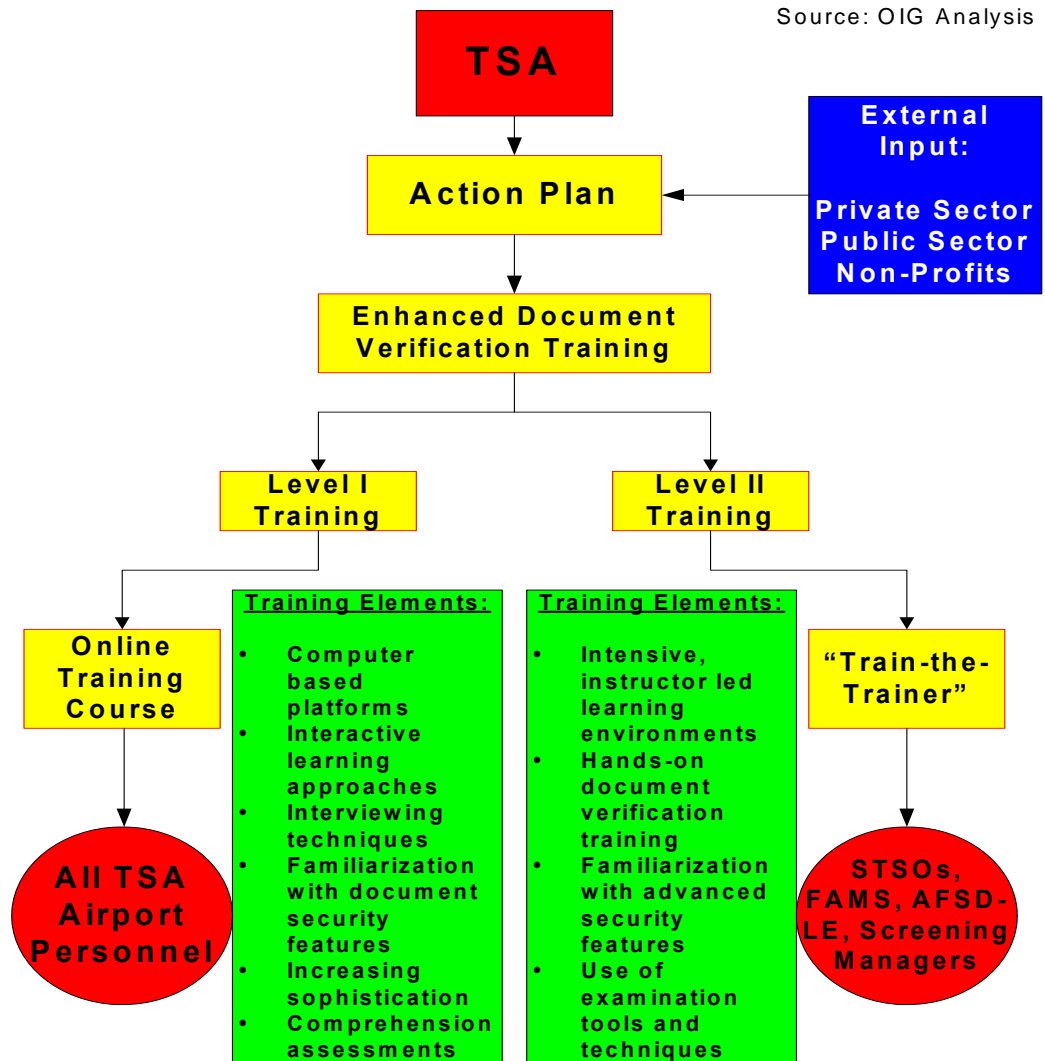
From May 2007 through June 2007, Baltimore/Washington International Airport in Maryland and Phoenix International Airport in Arizona incorporated best practices and technology into their checkpoint screening operations as phase one of this pilot program. TSA reported that John F. Kennedy International Airport in New York has also initiated this pilot.



While the training associated with this pilot is a good start, TSA should also begin enhancing its document verification training through the development

of a two-level document verification and training system. This would improve TSA's ability to verify the authenticity of travel documents. A two-level system would allow TSA to train all of its TSOs in basic verification techniques, while providing advanced training for law enforcement and other management personnel. Level I training should incorporate a more complete and interactive online training approach than what is available through TSA's Online Learning Center. Level II training should feature an instructor-led "train-the-trainer" program, which provides for more hands-on experience with specific identification methods to verify unique security features contained in identity documents, which could then be further disseminated across TSA. In Figure 8, we diagram training elements that TSA should consider when developing and implementing an action plan to address deficiencies in TSO document verification training. TSA could better develop document-verification training by soliciting input and assistance from various public, private, and nonprofit entities with expertise in this area.

Figure 8: Document Verification Training Elements



## Recommendations

We recommend that the Assistant Secretary for TSA:

**Recommendation #4:** Ensure that exit lanes are included in the travel document checker operating procedures, and that a second form of government issued photo identification is routinely being reviewed at all exit lanes.

**Recommendation #5:** Develop an enhanced two-level document verification training system for TSA personnel that encompass basic and advanced techniques to identify security features contained in government issued photo identification documents.

## **Management Comments and OIG Analysis**

**TSA Response:** TSA concurred with Recommendation 4. In their response TSA management stated that revised language, to include the "exit lane monitor" in travel document checking procedures, has been approved and will be implemented in the next revision of the Screening Management standard operating procedure, which is scheduled for release in the spring of 2008. TSA management also added that checking a second form of government-issued photo identification is a current requirement in the Screening Management standard operating procedure.

**OIG Analysis:** We consider TSA's actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until TSA provides us with a copy of the revised Screening Management standard operating procedure which includes the revised language.

**TSA Response:** TSA concurred with Recommendation 5, and said the two-level document verification training system was implemented in early fiscal year 2008. The training consists of five hours of on-line training and three hours of classroom training with scenarios and on the job training. Training is required for anyone performing Travel Document Checking. TSA management added that TSA training instructors were used to train the trainers to rollout the Travel Document Checking during the nationwide rollout to all federalized airports from October 2007 to March 2008.

**OIG Analysis:** We consider TSA's actions responsive to the intent of the recommendation, which is resolved and closed. No further reporting is necessary.



### **TSA Should Conduct Tests to Evaluate the LEO Check-In Process**

Officials from all levels of TSA, as well as from the law enforcement community, described the LEO flying armed check-in process as a vulnerable aspect of aviation security. However, TSA has not taken any steps to quantify how susceptible this vulnerability is to compromise.

TSA conducts various internal security tests at airports to include passenger screening, checked baggage, airport access doors to the sterile and other restricted areas, and access to aircraft, but the exit lane procedures at screening checkpoints are not tested. TSA's Office of Inspection should develop procedures for covertly testing the LEO check-in process and the screening procedures at airport exit lanes. These tests should evaluate an airport's security protocols and adherence to TSA's standard operating procedures. Where TSA identifies vulnerabilities, it should devise and implement mitigation efforts and strategies.

### **Recommendations**

We recommend that the Assistant Secretary for TSA:

**Recommendation #6:** Revise covert testing protocols to include testing of law enforcement officer commercial airline-ticketing agent check-in and exit lane procedures to gain access to airport sterile areas.

### **Management Comments and OIG Analysis**

**TSA Response:** TSA concurred with Recommendation 6. In its response, TSA noted that the Office of Inspection's "Access Testing Plan" for the second quarter of fiscal year 2008 will increase access control testing scenarios at airports. TSA also responded that new vulnerability testing scenarios, designed to introduce improvised explosive devices into sterile areas, will include false boarding passes, false government issued identification, false Secure Identification Display Area badges and false law enforcement credentials.

**OIG Analysis:** We consider TSA's proposed actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until TSA provides us with documentation that the new vulnerability testing scenarios, which include false boarding passes, false

government issued identification, false Secure Identification Display Area badges and false law enforcement credentials, have been incorporated into the Access Testing Plan.

### **Inconsistent Application of Policies Further Complicate the Flying Armed Process**

One concern federal, state, and local LEOs raised to us was the use of different TSA logbooks at airport checkpoints across the country. They said that different logbooks add confusion to the process. We also determined that using different logbooks contributes to inaccurate completion of the forms. TSA's standard operating procedures require the Security Manager to maintain a logbook at the screening checkpoint that provides a written record of individuals who bypass the standard passenger screening process. According to these procedures, the logbook must contain the following information regarding an armed individual:

- Date and Time of Entry Into the Sterile Area,
- Full Name as it Appears on the Credential,
- Badge/Credential Number,
- Agency/Service/Department/Company,
- Address and Phone Number of His or Her Assigned Duty Station,
- Aircraft Operator Name and Flight Number,
- Identity of Individual in Custody or Under Protective Escort,
- Signature of the Individual Flying Armed, and
- Initials of the Designated TSA Representative Who Inspected the Credentials.

We reviewed the checkpoint logbooks from four of the airports we visited and determined the logbooks use different formats but contained the required information. However, it was difficult to determine whether any information was absent given that pages are not numbered or dated. We also note that some checkpoint logbooks are illegible and information was sometimes missing. For, example, a federal LEO did not provide his signature or agency's address and telephone number, while another federal LEO did not provide his agency's address, telephone number, or his flight information.

The checkpoint logbook used by Dulles International Airport in Virginia was the most effective. Unlike the other logbooks, the Dulles logbook is dated and clearly groups different LEO's together, i.e. federal, state, and locals, along

with providing for a separate logbook for Federal Flight Deck Officers. Federal Flight Deck Officers are airline pilots, navigators, and flight engineers authorized to carry a firearm aboard a commercial airline. Separate checkpoint logbooks help ensure that each group fills out completely all the necessary information, while also ensuring that the specific information is more readily accessible. We also note that TSA employees or airport police officers at the Baltimore/Washington International Airport in Maryland not only provide their initials but also provide their Secure Identification Display Access number, i.e. their badge number, on the logbook when processing a LEO into the sterile area.

## Recommendations

We recommend that the Assistant Secretary for TSA:

**Recommendation #7:** Revise operating procedures to ensure that Transportation Security Officers and airport police use a standard logbook to record law enforcement officer access to airport sterile areas. Each page of the logbook should be dated and sequentially numbered, and should require TSA employees or airport police officers to initial and record their Secure Identification Display Access number or badge number before allowing a law enforcement officer into the sterile area.

## Management Comments and OIG Analysis

**TSA Response:** TSA concurred with Recommendation 7. In their response, TSA management stated that a standardized Checkpoint Sign-In Log/LEO was implemented TSA-wide on March 15, 2008. The log was developed by TSA's Office of Law Enforcement/Federal Air Marshal Service and contains all of our recommended information.

**OIG Analysis:** We consider TSA's actions responsive to the recommendation, which is resolved and closed. No further reporting is necessary.

### **Flying Armed Training Needs Improvement and Better Internal Controls**

TSA's Office of Law Enforcement/Federal Air Marshal Service and the Office of Security Operations have responsibility for the Law Enforcement Officers Flying Armed program. There are several opportunities to enhance

and strengthen the flying armed program. For example, state and local LEO training is mostly provided by state and local academies and training centers. The flying armed training these facilities conduct is to adhere to valid training materials provided by TSA. TSA provides these materials to state and local law enforcement organizations via email, compact disc, or through the Department of Justice's Federal Bureau of Investigation law enforcement secure internet site, LEO.gov. This training can vary according to location, certain parameters as outlined by TSA, and the U.S. Code of Federal Regulations. However, there is also no current requirement for officers to receive any refresher training after having completed the initial training.

In our discussions with a number of state and local government officials, it is evident that the manner in which different agencies administer the flying armed training varies greatly. In March 2007, TSA updated the flying armed training information. The training covers the requirements for flying armed, as well as the process for transiting through security to access an airport's sterile area while armed.

TSA Assistant Federal Security Directors for Law Enforcement and Federal Air Marshal Special-Agents-in-Charge also distribute the flying armed training to state and local police departments. However, state and local departments are responsible for administering the flying armed training to their officers. During the commercial airline carrier check-in process, the officer will then self-certify that they have completed the training. TSA must rely on the good faith and professionalism of LEOs because there is no current method to verify that an officer has completed the training. The U.S. Code of Federal Regulations does not require either TSA or local departments to keep any records that identify who has completed the training.

Each state and local department we spoke with use a different means to administer and track the training. One officer who routinely travels armed said he had not taken the training since his initial processing at the local police academy, approximately 26 years ago. We observed that another department had a printout of the training, which was available to all officers who would be flying armed, accompanied by a list of officers that had taken the training. This department instructed each officer to review the training once before their first experience flying armed, and then to annotate the log-sheet to certify that he or she had been trained. Another department assigned an officer as their flying armed training coordinator. Based on the training provided by TSA, the officer developed an instructor-led course to administer the training. The course included a graded exam, which officers must pass

before the department will certify them to fly armed. The training coordinator keeps a record of those certified, as does that department's chief of police.

Since TSA's Federal Air Marshal Service assumed responsibility for the flying armed training program in October 2005, the accessibility of the program has improved. The Federal Air Marshal Service made the training available to more agencies to improve overall LEO compliance with the Code of Federal Regulations. However, several federal, state, and local officers we spoke with said they would welcome additional training, including some practical instruction. While requiring practical training in the future remains unlikely, the flying armed training should move beyond reiterating the requirements set forth in the U.S. Code of Federal Regulations, and concentrate on more operational concerns that a LEO might face while in the aviation environment.

## Recommendations

We recommend that the Assistant Secretary for TSA:

**Recommendation #8:** Petition for a change to the U.S. Code of Federal Regulations, which would require refresher training, on a cyclical basis, for all law enforcement officers flying armed. The change should also require that all law enforcement departments maintain records of such training.

## Management Comments and OIG Analysis

**TSA Response:** TSA concurred with this recommendation. TSA supports the concept of a LEO flying armed refresher training element. TSA has completed an initial draft amendment to the existing federal LEO flying armed regulation, which includes a requirement for refresher training on regular basis.

**OIG Analysis:** We consider TSA's proposed actions responsive to the recommendation. The recommendation is resolved and open. This recommendation will remain open pending our receipt of documentation of the change to the existing federal LEO flying armed regulation.

## **Improper Efforts to Influence Covert Testing Results Exist**

### **TSA's Internal Covert Testing Was Compromised But Advance Notification Is Not Pervasive**

During our visit to JAN, we determined that TSOs received notification of TSA's internal covert testing before the covert team began their test at the airport. We also interviewed TSA personnel at five other federalized airports to determine how they handled covert testing. At the five other airports, TSA management conveyed a desire for undistorted testing results as a means to gauge their airport's performance accurately. As TSA noted in its response to the report, these tests are not designed to be performance measures. Rather, they are evaluations of system vulnerabilities that can be used to design countermeasures.

In addition to discussions with local TSA management, we spoke with a number of TSA employees who had been part of covert testing at each of the airports we visited. The vast majority of employees said that they had no prior knowledge about any testing at the airport. Two employees at two different airports reported that they remembered hearing something about covert testing. One said that she heard the "red team" was in the region, while another said he heard the team would be "coming through" shortly. However, neither employee said this information came from TSA upper management, and no other employees at either airport corroborated this information. Also, there was no evidence that TSA's Office of Inspection improperly disclosed any advanced information.

TSA headquarters officials informed us that since 2002, there have been only two incidents concerning the improper disclosure of TSA internal covert testing information, excluding JAN and one incident concerning the improper disclosure of another government agency's covert testing. Given these few occurrences, we have determined that the improper disclosure of TSA internal covert testing information is not a systematic problem nor pervasive throughout TSA.

### **Jackson-Evers International Airport TSOs Received Advanced Notification of TSA Internal Covert Testing**

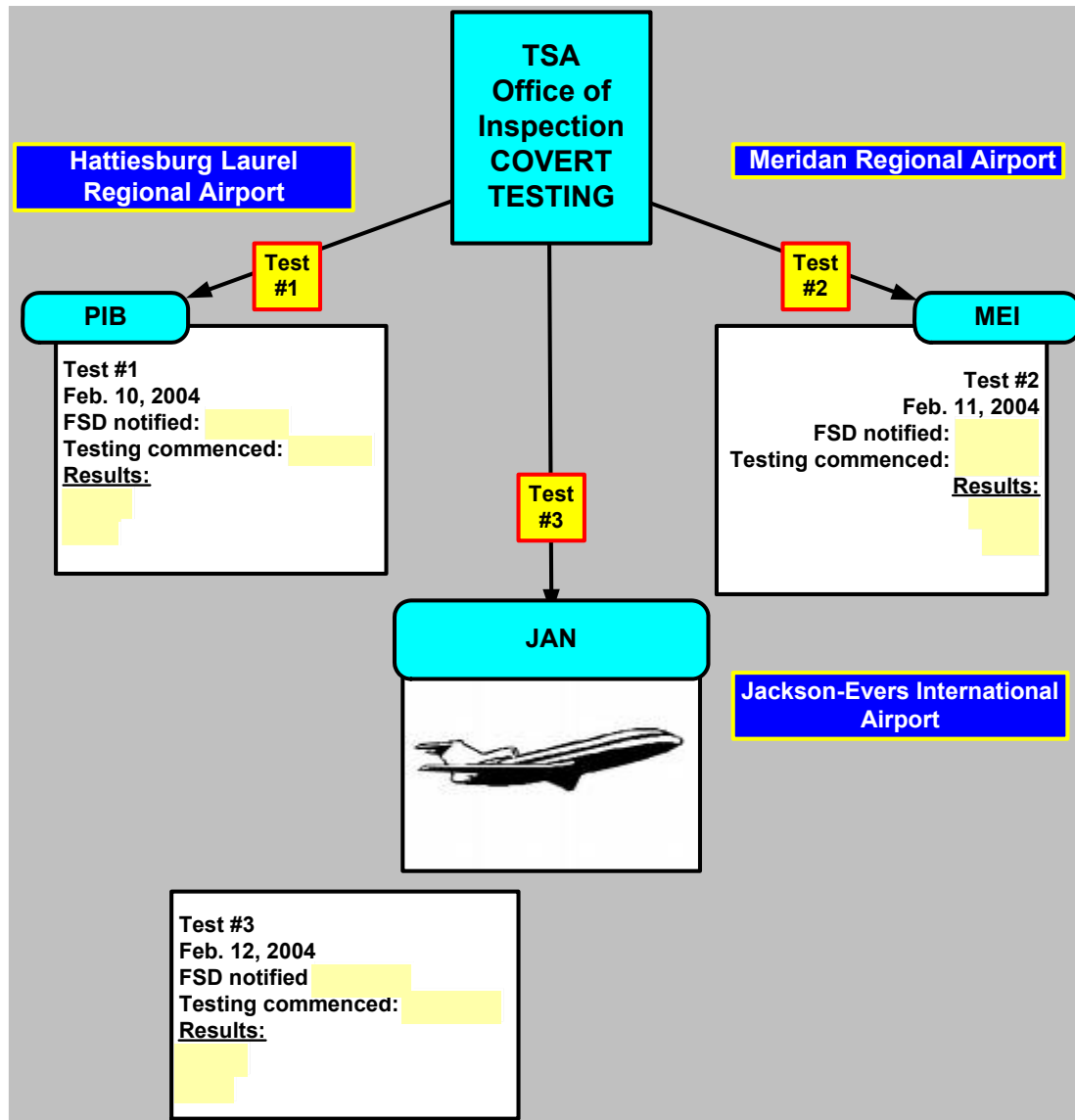
TSA conducted covert testing at JAN on February 12, 2004. They conducted five tests between JAN's two passenger screening checkpoints, beginning at 11:15 am, and [REDACTED] checked baggage screening. Each of the five tests

SENSITIVE SECURITY INFORMATION

**TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports**

## Appendix G

### Timeline of Covert Testing at Jackson-Evers International Airport





We could not identify with absolute certainty where the information first originated, but TSA management personnel at JAN communicated this information to certain individuals at all levels of TSA personnel at JAN. While management officials provided two alternate explanations regarding how the TSA internal testing might have been compromised, we determined each to be implausible.

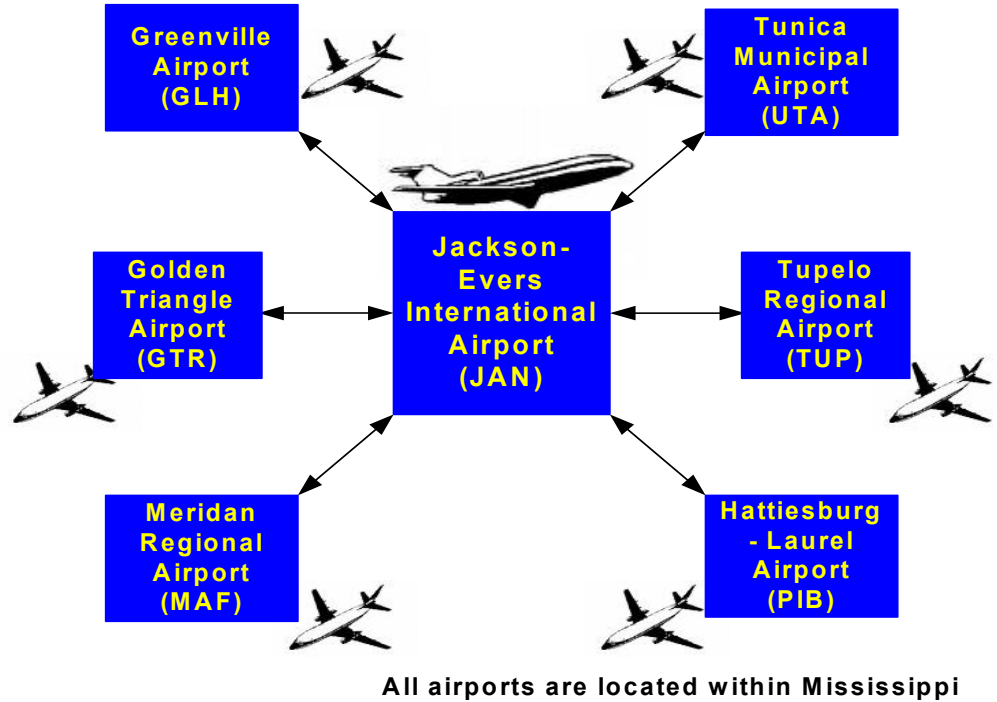
**Management's Efforts to Account For Compromised JAN Covert Tests Were Not Credible**

We spoke with all levels of JAN management concerning these allegations, including the acting Federal Security Director, Assistant Federal Security Directors, and Security Managers. JAN management provided two general explanations as to how the TSA internal covert tests could have been comprised. We determined that neither was credible.

The first explanation, offered by senior management at JAN, suggested that TSOs from one of JAN's spoke airports might have passed along information about covert testing to JAN personnel. With over 450 federalized airports, TSA has established a reporting and management structure around a series of hub-spoke airport alignments that allows larger airports, or hubs, to oversee the field operations of smaller airports, or spokes, in close geographic proximity. The following figure illustrates the hub-spoke airport alignment at JAN.



**Figure 10: TSA Hub-Spoke Airport Alignment at JAN**



As depicted in Appendix G, TSA tested two of JAN’s spoke airports in succession on February 10 and 11, 2004: Hattiesburg-Laurel Regional Airport and Meridan Regional Airport, both in Mississippi. JAN management said TSOs from either Hattiesburg or Meridan could have passed along information about covert testing to TSOs from JAN because management immediately sent TSOs from each airport to JAN for remedial training. Because TSOs are required to complete such training before they can resume certain screening duties, management said that TSOs from each spoke would have interacted with JAN personnel before February 12, 2004.

The second explanation offered by TSA middle management at JAN suggested that any information relayed to TSOs was done in the spirit of “training,” not to compromise future covert testing.

Again, as the hub for Hattiesburg and Meridan, JAN management knew about the TSA internal covert testing at each airport per TSA’s standard operating procedures. However, management was obligated not to disseminate that information. This is established by TSA’s Office of Inspection during their

initial discussion with the airport's Federal Security Director, during its post-test out-briefs, and underscored by its Nondisclosure Agreement, which states that all information concerning covert testing is Sensitive Security Information and "may not be released to persons without a *need to know*..." TSOs who were subject to future covert tests were not in a need-to-know position.

While TSOs from either spoke airport could have passed along information to TSOs from JAN, this does not account for why management specifically conveyed sensitive information to TSOs via oral briefings, or why they purposefully heightened the awareness of TSOs on the day of the test through their unusual physical presence at JAN's checkpoints. Furthermore, any rationale that such information was to be used for "training" purposes, despite that JAN had not yet been tested, underscores the reality that management hoped to use this information to improve the results of impending covert testing at JAN.

JAN management deliberately engaged in improper efforts to artificially improve covert testing results because they were concerned about perceptions associated with poor performance. Their efforts not only distorted the results for JAN, but also negated those results as a point of comparison among other airports that TSA internally tested during the initial period. These compromises prevented TSA's Office of Inspection from accurately assessing JAN's safety and security posture.

### **TSA's Field Management Views Covert Testing As Useful Tool**

Every management official we spoke with at the five other airports expressed a desire for unbiased covert testing results. They viewed covert testing as a positive tool for assessing performance, without punitive implications. One Federal Security Director said that he views covert testing as an opportunity to modify their airport's internal training protocols. For instance, should his airport fail a covert test because of an improper screening, management could later reemphasize the proper screening procedures during future training.

Another Federal Security Director said that after receiving a call from TSA's Office of Inspection's internal covert team about an impending test at a spoke airport, he requested that they also test his hub and another spoke. This additional testing provided the director with a better understanding of how the majority of his airports were functioning.

To ensure the integrity of the covert testing process, management officials at these airports even took steps to ensure that personnel did not compromise the tests, including withholding this information from a Deputy Federal Security Director, if necessary. At one airport, a TSO detailed to the airport's security operations center said that management informed the center that tests were about to occur, for operation and situational awareness, but the operations center was specifically instructed not to disseminate any information.

### **External Covert Testing Conducted by Our Office Was Compromised**

At the request of Chairman Bennie G. Thompson, we expanded our review in November 2007 and initiated an investigation into the circumstances surrounding an email, purportedly sent by the Assistant Administrator of TSA's Office of Security Operations on April 28, 2006, which may have compromised covert government testing of TSA airport screening checkpoints in 2006. A copy of the November 1, 2007, request letter is in Appendix H, and a copy of the April 28, 2006, email is in Appendix I.

Our Office of Audits team conducted covert security testing at the Jacksonville International Airport, in Jacksonville, Florida on April 27, 2006, and April 28, 2006. Jacksonville was the third airport test location in our initiative to test 14 airports nationwide during April 24, 2006, through July 14, 2006. The first airports tested were the Charleston International Airport, in Charleston, South Carolina on April 24, 2006, and the Savannah International Airport, in Savannah, Georgia, on April 26, 2006. The covert testing we performed in 2006 tested Airport Access Control Systems, which are primarily under the control of entities within the airline industry, such as commercial airline carriers and airport authorities, not TSA.

Our investigation disclosed that an April 28, 2006, email provided key details about our covert airport security testing program, including our test methodology and the physical description of one of our undercover testers. We determined that airline security representatives created the email and forwarded it to TSA officials, who then broadcast the message to approximately 388 users of the TSA NETHUB email system. NETHUB is a division within TSA's Office of Security Operations that serves as a central communications conduit between TSA headquarters and TSA field operations at more than 400 airports. NETHUB sends and receives communications by email, telephone, and fax on operational and administrative matters, such as distributing new screening procedures and security directives.

We interviewed the former Acting Assistant General Manager of NETHUB who stated that on April 28, 2006, he received an email from the Federal Security Director in Minneapolis-St. Paul, Minnesota, titled "TEST WARNING," which contained notices between airport directors describing tests of airport security procedures. The NETHUB Acting Assistant General Manager claimed that he interpreted the messages as identifying possible unauthorized testing by nongovernment entities. The NETHUB Acting Assistant General Manager said he immediately brought the email to the Special Assistant for the Assistant Administrator of TSA's Office of Security Operations and requested approval to forward the information to the field.

We determined the message was renamed "NOTICE OF POSSIBLE SECURITY TEST" and sent from TSA's NETHUB communication system on April 28, 2006, at 2:51 p.m. The email is as follows.

"This information is provided for your situational awareness. Several airport authorities and airport police departments have recently received informal notice of possible DOT/FAA security testing at airports around the nation. Here is the text of one such notification:

Several airports have reported that the DOT is testing airports throughout the country. Two individuals have been identified as FAA or DOT at the airport in JAX this morning. They have a stack of fake ID's, they try to penetrate security, place IED's on aircraft and test gate staff. These individuals were in CHS earlier this week and using a date altered boarding pass managed to get through the security checkpoint. Alert your security line vendors to be aware of subtle alterations to date info. They should also pay very close attention to the photo id's being presented. They will print a boarding pass from a flight, change the date, get through security (if not noticed) and try to board a flight and place a bag in the overhead. There is a couple, and the woman has an ID with an oriental woman's picture, even though she is Caucasian. We are getting the word out.

Office of Security Operation, NetHub"

Although we determined that the Assistant Administrator of TSA's Office of Security Operations did not approve the April 28, 2006, NETHUB email

message broadcast, and actually took steps to recall it within 14 minutes; he failed to notify us of the compromise, potentially undermining the integrity of our ongoing covert testing at 11 additional airports. We also determined that several other senior TSA officials, including TSA's liaison to our covert testing team, knew about the email but failed to notify us of the compromise.

TSA responded that it has an excellent track record of cooperation with our office and with the Government Accountability Office in relation to covert testing by those offices. Further, TSA said that we and the Government Accountability Office have tested TSA operations on a regular basis for the last five years without any evidence of a compromise in test integrity created by a TSA employee.

Our investigation confirmed that TSA officials sent the email advising its Federal Security Directors and others of covert government airport testing. The email revealed details about our testing methodology and provided tester descriptions that compromised the testing procedures. The fact that the Assistant Administrator recalled the message is evidence that the message was inappropriate. However, there was no follow up with email recipients, and no effort to contact us to report the compromise. TSA officials who reported believing the email to be "unauthorized probing," are not credible in light of the details provided in the email. Further, there is no record of any attempt by TSA personnel to notify any appropriate law enforcement agency, including divisions within TSA, that unknown individuals were testing airport security.

TSA's disclosure of our covert testing procedures was inappropriate and interfered with a legitimate function of our office. Further, at no time did any TSA official inform us that our testing methodology was compromised. Improvements are needed to both TSA's internal covert testing program and the advance notification of covert testing conducted by our office, as well as the process for reporting possible compromise. These deficiencies create vulnerabilities in TSA's layered security approach and prevent us from accurately assessing TSA's safety and security posture.

## **Covert Testing Procedures Can Be Further Strengthened**

Since 2005, TSA's Office of Inspection has undertaken several steps to improve the operational effectiveness of its internal covert testing program. These improvements have allowed the Office of Inspection to adjust its testing methodologies to ensure greater testing integrity. However, TSA can further

~~SENSITIVE SECURITY INFORMATION~~

**TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports**

strengthen its procedures to ensure greater operational security by stressing the importance of the covert testing program and reiterate the penalties for unauthorized disclosures.

### **TSA Has Improved Its Covert Testing**

TSA's Office of Inspection, Special Operations assumed responsibility for all TSA internally conducted covert testing in early 2002. Before this time, the Federal Aviation Administration had this responsibility. Beginning in November 2002, TSA's Office of Inspection set out to test every federalized airport within three years, and resumed testing using concealed knives, firearms, and fully assembled Modular Bomb sets. By 2003, TSA began using simulated next-generation improvised explosive devices and gradually began introducing more complicated concealment techniques during testing.

From 2004 through the present, TSA adopted a risk-based approach to internal covert testing that is largely intelligence-driven and intended to mimic real-world situations. This real-world approach incorporates artful concealment, and other techniques intended to increasingly challenge TSOs during the covert testing process.

The evolution of these testing articles coincides with an increase in the Office of Inspection staffing and budget. In 2002, there were only five full-time employees dedicated to performing covert tests. By 2006, there were 22 full-time employees dedicated to performing TSA's covert testing. TSA also began to supplement its covert testing teams with other TSA personnel to improve operational effectiveness. More staff allows the Office of Inspection to perform additional internal covert tests of different terminals at the same airport simultaneously.

For FY 2003, the overall budget for TSA's Office of Inspection was approximately \$12 million; by FY 2007, its budget had increased to more than \$32 million. The growth allowed TSA to stop the practice of testing hub-spoke or proximate airports in close succession, which reduces the likelihood that airports would be aware that they might be subject to an impending TSA internal covert test.

[REDACTED]

[REDACTED]

TSA internal covert testing is about to begin. The protocols also note that the director should refrain from notifying TSA managers or supervisors of the test.

[REDACTED]

We agree with TSA's decision to notify the local airport police and the Federal Security Director. However, as the on-site authority responsible for managing a crisis, the Federal Security Director should also be subject to covert testing as are other TSA employees.

[REDACTED]

The purpose of covert testing is to discreetly evaluate system vulnerabilities that can be used to design countermeasures. Those intent on circumventing the screening process are looking to exploit any weakness, and will look to take advantage of periods when the system is under tremendous stress, be it during such special circumstances, or due to personnel, mechanical, weather-related, or procedural difficulties.

In addition to TSA, our Office of Audits also conducts covert testing of aviation security, as does the Government Accountability Office. While we use different protocols than TSA's Office of Inspection, we have determined that our Office of Audits will continue its practice of advance notification. Specifically, we believe it prudent to continue providing the Federal Security Directors with advance notification of our covert testing because we are not a part of TSA's internal reporting structure and want to afford the directors this courtesy, in an effort to avoid potential conflicts with airport operations. However, TSA should afford us the same courtesy it requests of its Federal Security Directors to refrain from notifying TSA managers or supervisors of covert testing. Providing advanced notification not only distorts testing results, but also negates those results as a point of comparison among airports.



These compromises prevent us and TSA's Office of Inspection from accurately assessing TSA's safety and security posture.

## Recommendations

We recommend that the Assistant Secretary for TSA:

**Recommendation #9:** Annually disseminate a letter to all TSA airport security personnel that stresses the importance of the covert testing program and reiterates the penalties for unauthorized disclosures, whether tests are conducted by TSA's Office of Inspection or the Office of Inspector General.

## Management Comments and OIG Analysis

**TSA Response:** TSA concurred with this recommendation. In its response, TSA stated that they will take actions to reinforce the importance of protecting covert test integrity. TSA management also stated that the expectations with respect to the proper handling of information have been clear within TSA. The TSA Online Learning Center currently includes an online training course on Sensitive Security Information. In addition, TSA annually has a "Sensitive Security Information Awareness Week" at all TSA facilities. In the future, TSA plans to incorporate the purpose of covert testing and the importance to safeguard covert test results into the awareness week activities.

**OIG Analysis:** We consider TSA's actions responsive to the recommendation. The recommendation is resolved and open. This recommendation will remain open pending our receipt of documentation that the purpose of covert testing and importance of safeguarding covert test results is incorporated in the "SSI Awareness Week" activities.

## TSA Can Improve Its Processes For Reporting Security Incidents

TSA can improve its processes for reporting the discovery of deadly, dangerous, or prohibited items. We determined that TSA personnel follow proper protocols when a TSO initiates the process to report an incident via the Performance and Results Information System and to the Freedom Center, when necessary. However, there are indications that TSOs have not reported some incidents as required. TSOs made those decisions out of fear of reprisal or because professional courtesies had been extended. Since personnel do not



report all incidents, information used to document trends and analyze incidents is incomplete.

### **Decisions Have Been Made Not to Report Certain Incidents**

We received indications that TSOs are not reporting some incidents despite requirements to do so. Non-reporting occurred in one of two ways. Either TSOs initially made the decision not to report an event, or management decided not to report the incident. TSOs said they did not report incidents for fear of losing their jobs or retaliation. TSOs at two airports we visited maintained personal logs of daily occurrences at their airports. Three TSOs promised to provide us with copies of their logs but later declined due to fear of retaliation.

In one incident, a TSO said that during a baggage search he failed to remove mace from a passenger's carry-on baggage at the checkpoint because of insufficient communication. The TSO said that he thought the baggage check was only for a bottle of water, which he removed. After the passenger cleared screening, another TSO working the X-ray machine asked if he had also removed the mace. He said he had not. The Supervisory TSO told the TSO to try to find the passenger in the airport's sterile area. When the TSO was unable to do so, both the TSO and Supervisory TSO disregarded the incident without any notification to the Federal Security Director, a Security Manager, or the airport police. As mace is a prohibited item, the incident is required to be reported, and could have resulted in the sterile area being cleared and passengers being rescreened. The TSO said he went along with the Supervisory TSO's decision because he did not want to lose his job for failing to prevent the prohibited item from entering the sterile area.

We are concerned that some TSOs at the airports we visited expressed the reason they had not reported an incident was out of a fear of retaliation by local TSA officials at those airports. We discussed with these TSOs the protocols for documenting incidents they believed required reporting to TSA's Ombudsman, its Office of Inspection, or our Office of Investigations, but were not. The TSOs said they had lost faith in the processes because past complaints concerning inconsistently followed aviation security procedures and protocols had resulted, in their view, in retaliation by supervisors. Although these concerns are not within the scope of this review, we are pursuing additional work in these areas. Furthermore, TSA should work to resolve the concerns expressed by its TSOs, particularly when the potential

fear of retaliation overshadows operational requirements to document security incidents.

### **Professional Courtesies Have Been Extended to LEOs**

Extending professional courtesies to armed LEOs has resulted in inconsistent application of TSA standard operating procedures relating to carrying firearms, and confusion on the part of TSOs. These discrepancies contribute to weakening TSA's layered commercial aviation security approach.

TSOs reported that LEOs have received professional courtesies after improperly trying to pass through security checkpoints with a firearm. While Supervisory TSOs and airport police officers do respond when a TSO discovers a firearm at the checkpoint, TSA personnel and airport police have allowed LEOs to carry their firearms back to their vehicles; and in some cases have even held firearms until LEOs can retrieve the weapon upon return to the airport. It is unlikely that either TSA personnel or airport police would afford an ordinary citizen similar courtesies. Rather, after going through the appropriate checks, the citizen is typically subject to a civil penalty. As required by directive OD-400-18-1 – *Reporting Security Incidents via the Performance and Results Information System*, TSA personnel must report all incidents involving the weapon of a law enforcement officer through the Performance and Results Information System. Directive OD-400-18-2B – *Reporting Security Incidents to the Transportation Security Operations Center*, also states that incidents involving the weapon of a law enforcement officer require immediate telephonic notification to the Freedom Center.

An Assistant Federal Security Director for Regulatory said that he had two incidents involving LEOs bringing firearms to the checkpoint. TSA closed both cases administratively by issuing a warning letter to the LEOs. When asked, the assistant director said that should either be involved in a similar incident again, TSA would issue a civil penalty, as a second offense, and the LEOs would be unable to claim that they did not know their responsibilities. Without formally recording each incident, regardless of who is involved, TSOs will lose confidence in a process and perceive it as being unfair, particularly if it undermines their authority.

## **TSA Should Consider Certain Best Practices**

During our review, we identified best practices in use or planned at various airports that TSA should consider replicating at all federalized airports. We define a best practice as the most efficient, effective, and economic way of accomplishing a task, based on repeatable procedures that have proven themselves over time. The best practices observed include the use of operations centers, and enhanced educational and outreach opportunities and additional training for TSOs. Should TSA implement these practices nationwide, we believe they will yield improved efficiencies in the discovery and reporting of security incidents.

### **Operations Centers Are Useful Resources For Incident Reporting**

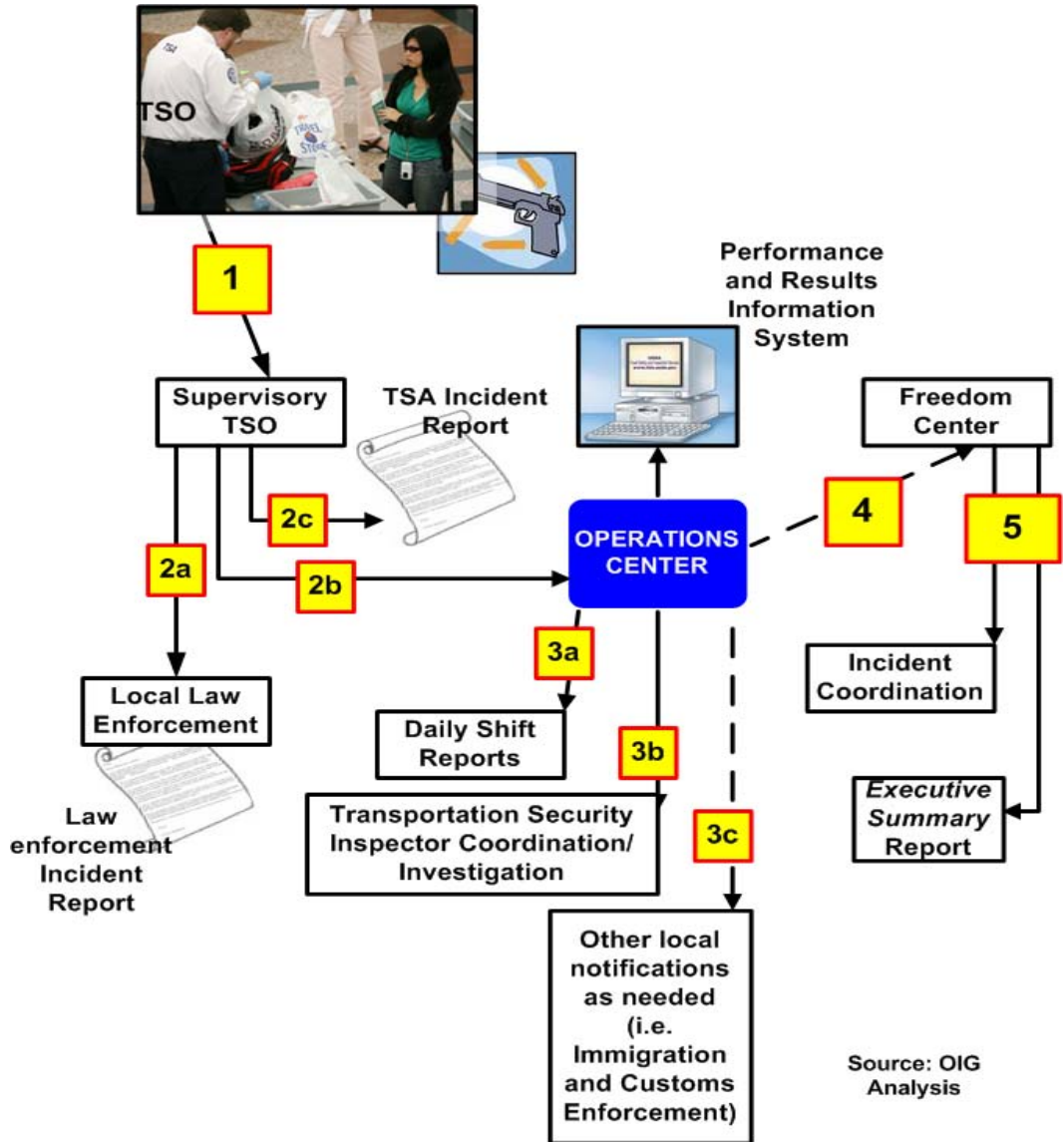
Five of the six airports we visited, Baltimore/Washington International Airport, Charlotte-Douglass International Airport, Dulles International Airport, Lubbock International Airport, and Ronald Reagan Washington National Airport, use an operations center as the central repository for all incident information. These centers function as the notification and clearinghouse for all incidents that occur at the airport. Operation centers at larger airports such as Baltimore/Washington International Airport are very common. However, smaller airports like Lubbock International Airport do not always have operation centers. TSA personnel said that an operations center is essential to efficient and effective reporting of incidents.

When we visited the Lubbock International Airport in Texas, we learned that local TSA management had set up the West Texas Communications Center. At some airports, the terms “communications center” and “operations center” are used interchangeably. TSA management at Lubbock noticed TSOs had to manage a variety of situations that required notification to various agencies and those notifications often required completing a huge amount of paperwork. As handling notifications and paperwork was a burden for TSOs, TSA management at Lubbock created the West Texas Communication Center. This operations center has standardized the reporting process and allowed TSOs to concentrate on screening operations instead of documenting and following up on incidents that occur at the airport. Figure 11 depicts the process for reporting incidents through the West Texas Communications Center.

~~SENSITIVE SECURITY INFORMATION~~

**TSA’s Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports**

Figure 11: West Texas Communications Center Reporting Process



The Federal Security Director staffs the operations center with TSOs on six-month details; and TSOs are required to maintain their certification during this period. A Security Manager said that the operations center acts as the hub for all reporting from its five spoke airports. It ensures that TSA personnel properly report all incidents. A Supervisory TSO further said that having the operations center allows them to quickly return their focus to checkpoint operations, instead of having to make calls to the Freedom Center or follow-

up on other reporting requirements. Another Supervisory TSO said that the operations center is an excellent program. He said a supervisor is very busy, and the operations center relieves some of the stress so supervisors can work the incident and let someone else worry about the reporting. He added that the operations center staff are meticulous, and there are no inquiries coming back from the Freedom Center requesting additional information.

## **Recommendations**

We recommend that the Assistant Secretary for TSA:

**Recommendation #10:** Require all hub airports to create operation centers, or another centralized reporting procedure, for collecting and reporting the required information for the Freedom Center and Performance and Results Information System for all hub-and-spoke aligned airports.

## **Management Comments and OIG Analysis**

**TSA Response:** TSA concurred with this recommendation. In its response, TSA stated that Operations Directive (OD)-400-30-10, Coordination Center Requirements and Functions, was issued in January 2008. This Directive establishes 122 Coordination Centers strategically placed in airports throughout the United States. One of the core functions of the Coordination Center is to streamline and standardize reporting of security incidents to TSA's Freedom Center which is TSA's central point for reporting. For the centers, 100 of the 122 centers are in operation with the remaining 22 slated to be established by July 1, 2008.

**OIG Analysis:** We consider TSA's actions responsive to the recommendation, which is resolved and open. This recommendation will remain open pending our receipt of documentation regarding the Operations Directive and verification that the 122 Coordination Centers have been established.

### **Additional Educational and Outreach Opportunities Should Be Provided to TSOs**

Most of the TSOs we spoke with are not aware of how the entire discovery and reporting process functions, or the penalties associated with an individual who brings a dangerous, deadly, or prohibited item to a checkpoint. TSOs

said that after they discovered a person with a firearm, the individual would later return to the checkpoint and continue with their travel arrangements. Some TSOs seemed frustrated that the local airport police did not arrest or detain the individuals. TSOs also said they are not aware of the regulatory process that levies civil penalties on individuals attempting to bring a firearm through a security checkpoint. Insufficient information and understanding of the discovery and reporting process, as well as the associated civil penalties that can be imposed, makes some TSOs believe their efforts are in vain and that they are not having an overall effect on commercial aviation security.

Conducting outreach and training sessions with the TSOs concerning the entire discovery and reporting process would give TSOs a better understanding of the entire process, which could have a positive effect on morale by encouraging TSOs to take more ownership of their role in the process. It will also serve to complete the information cycle or feedback loop. With greater awareness of how the regulatory process functions, TSA management could alleviate some TSO concerns, misgivings, and complaints.

## **Recommendations**

We recommend that the Assistant Secretary for TSA:

**Recommendation #11:** Develop a strategy for and conduct outreach to support all Transportation Security Officers knowledge and understanding of incident discovery, reporting, and enforcement processes.

## **Management Comments and OIG Analysis**

**TSA Response:** TSA concurred with this recommendation. In its response, TSA Management stated that all TSOs are required to complete training developed by the Office of Compliance – Performance and Results Information System Program and provided through TSA's Online Learning Center on incident discovery, reporting, and enforcement processes. The specific name of this course is Performance and Results Information System Online Learning Center Incident Reporting Training.

**OIG Analysis:** We consider TSA's actions responsive to our recommendation. The recommendation is resolved and open. This recommendation will remain open until TSA provides us with documentation of the training developed by the Office of Compliance – Performance and



Results Information System Program and the course entitled, Performance and Results Information System Online Learning Center Incident Reporting Training.

### **Incident Report Training and Information Should Be Provided to TSOs**

We determined that most TSOs are not aware of the entire reporting and enforcement processes involved in reporting incidents. They are not aware of the type of information that Transportation Security Inspectors need to conduct a thorough investigation of a dangerous or deadly item discovered at a checkpoint.

During our visit to one airport, an Assistant Federal Security Director for Regulatory said it could be difficult for Transportation Security Inspectors to effectively conduct investigations since they are not typically on the scene when an incident occurs. Inspectors must rely on TSOs to gather certain information, such as pictures of the dangerous or deadly item and the subject's information, which is crucial to the civil enforcement process. A Transportation Security Inspector said that not being located at the airport when an incident is reported can hinder an investigation, because different TSOs might provide different accounts of an incident, which would sometimes force the inspector to reinterview individuals who might have been involved in the incident. The Transportation Security Inspector added that a report-writing course for TSOs that addresses what an incident report should cover would be helpful and would allow TSOs to perform their jobs better. As the need for accurate incident information is necessary for inspectors to know how to proceed with a case, TSOs who are more aware of the report-writing process and its requirements should facilitate such investigations.

A Transportation Security Inspector at another airport we visited is developing a training course for TSOs concerning report writing and the enforcement process. The inspector said that training would focus on how the information collected by TSOs affects the enforcement process. The training will include information discussing how a case is classified depending on the seriousness of the incident, the role of aggravating or mitigating circumstances involved, and the importance of ensuring that TSOs obtain accurate and complete identity information of the passenger.

## Recommendations

We recommend that the Assistant Secretary for TSA:

**Recommendation #12:** Develop and deliver training to all Transportation Security Officers on incident report writing.

## Management Comments and OIG Analysis

**TSA Response:** TSA concurred with this recommendation. In its response, TSA noted that training on incident report writing is included in the Performance and Results Information System Online Learning Center Incident Reporting Training. TSOs are required to obtain a certificate of successful completion for this course, prior to requesting access to the Performance and Results Information System application. The TSO's supervisor must confirm that the user has been properly trained in how to file reports in the system, before granting access. The current statistics show that more than 2,200 TSOs, reporting in Performance and Results Information System, have completed this training since its inception. The incident report training identifies processes involved in reporting security incidents and includes the types of information required by Transportation Security Inspectors to conduct a thorough investigation. Applying the training, the TSO is able to identify all pertinent details, without requiring an on-scene response by an Inspector.

**OIG Analysis:** We consider TSA's actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until TSA provides us with documentation of the Performance and Results Information System Online Learning Center Incident Reporting Training.



## Appendix A

### Purpose, Scope, and Methodology

---

We assessed TSA's management of its aviation security activities at the Jackson-Evers International Airport (JAN), in response to a congressional request from U.S. Representative Bennie Thompson, Chairman of the House Committee on Homeland Security. Our assessment focused on TSA's:

- Authorization of certain individuals to fly armed;
- Covert testing of its airport security operations; and
- The process of reporting security incidents that occur at an airport

To accomplish our objectives, we also reviewed the management of aviation security operations at five other airports, including Baltimore/Washington International Airport in Maryland, Charlotte-Douglass International Airport in North Carolina, Dulles International Airport in Virginia, Lubbock International Airport in Texas, and Ronald Reagan Washington National Airport in Virginia.

We chose three of the airports because they processed a large volume of individuals flying armed. We chose one airport because it closely mirrored the size and scope of operations at JAN. While every airport is unique, these additional site visits provided us with a better overall understanding of TSA operations with respect to these assessed areas.

At each airport, we met with relevant TSA field personnel, including the Federal Security Directors, the Assistant Federal Security Directors, Security Managers, and TSOs. We also met with a number of TSA's partners, including each airport authority and several commercial airline representatives. Each partner has some operational nexus to our three areas.

We interviewed more than 160 people including TSA personnel from TSA headquarters, the Office of Inspection, the Office of Law Enforcement, the Office of Security Operations, the Freedom Center, formerly the Transportation Security Operations Center, and TSOs in the field. We also spoke with personnel from U.S. Immigration and Customs Enforcement's Fraudulent Document Laboratory, Federal Law Enforcement Training Center, and DHS' Office of Operations Coordination and Planning.

We spoke with 43 LEOs from 17 different federal, state, and local law enforcement agencies. Each officer had experience dealing with the flying armed process.

~~SENSITIVE SECURITY INFORMATION~~

**TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports**

## Appendix A

### Purpose, Scope, and Methodology

---

We reviewed relevant laws, regulations, policies, procedures, statistical information, and airport practices related to these three areas. Given the size and scope of TSA's airport operations, we are not suggesting these issues are prevalent across TSA. However, we note some areas of concern that highlight the need for some systemic internal assessments.

Our fieldwork began in February 2007 and concluded in June 2007. At the request of Chairman Thompson, we expanded our review in November 2007 and investigated whether TSA compromised any covert testing by another federal government entity. The results of this investigation are included in this report. We initiated this review under the authority of the *Inspector General Act of 1978*, as amended, and according to the "Quality Standards for Inspections," issued by the President's Council of Integrity and Efficiency.

~~SENSITIVE SECURITY INFORMATION~~

**TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports**

**Page 54**

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.~~

## Appendix B Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

Office of the Assistant Secretary

U.S. Department of Homeland Security  
601 South 12th Street  
Arlington, VA 22202-4220

JUN 27 2008



Transportation  
Security  
Administration

### INFORMATION

MEMORANDUM FOR: Richard L. Skinner  
Inspector General

FROM: Kip Hawley *CH*  
Assistant Secretary

SUBJECT: Transportation Security Administration (TSA) response to  
Draft Report Entitled "Transportation Security  
Administration's Management of Aviation Security  
Activities at Jackson-Evers International and Other  
Selected Airports"

### Purpose

This memorandum constitutes TSA's response to Draft Report OIG-08-xx, April 2008, "Transportation Security Administration's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports."

### Important Correction Needed on NetHub Communication

The facts determined by OIG's investigation of purported tip-offs to its own covert testing completely exonerate TSA personnel from that allegation. The OIG report should highlight those facts since there was public discussion that, if left uncorrected, undermines TSA leadership in its important security responsibilities. For months, those unfounded allegations have hung over several dedicated career public servants who have made outstanding contributions to our nation's security and, while the public may have moved on, these men of integrity and their families and co-workers have been deeply hurt by the unfair and unfounded allegations.

The salient facts are:

- OIG conducted covert tests of airports— not TSA operations;
- Airport law enforcement spread the word about covert testing, not TSA;

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.

## Appendix B Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

2

- The NetHub message in question came a day AFTER the law enforcement alert on covert testing;
- A NetHub duty officer passed-on the law enforcement alert to TSA offices around the country – he did not intend it as a tip-off and had no knowledge about the true nature of the incidents being reported;
- It was determined that the Assistant Administrator of TSA's Office of Security Operations did not approve the April 28, 2006, Nethub email message broadcast, and actually took steps to recall it within 14 minutes; and
- There was at no time an intent from officials at TSA to tip-off covert testing.

TSA welcomes the thoughts by OIG that TSA should have taken the extra step to contact OIG after the alert went out and several other process matters. However, the facts simply do not support any negative conclusions about TSA's commitment or actions related to covert test integrity.

The facts clear the individuals involved and, in fairness, this report should as well.

### Background

In October 2006, the Department of Homeland Security (DHS) Office of the Inspector General (OIG) began a review of allegations that the security and integrity of the passenger screening process at the Jackson-Evers International Airport (JAN) was being compromised routinely by TSA employees. The scope of the review was later broadened to cover additional incidents related to JAN. As a result, OIG reports on four questions: (1) Did TSOs at JAN receive any advanced notice of internal TSA covert testing being conducted; (2) Did TSOs report the discovery of firearms and other dangerous or deadly items as required by TSA policies and directives; (3) Do existing processes, which authorize certain individuals to fly armed, need strengthening; and (4) Did TSA compromise any covert testing conducted by another Federal government entity?

OIG found that despite the progress made toward improving its internal covert testing, additional work is necessary. Specifically, OIG suggests that the TSA can take steps to improve security activities within commercial aviation by eliminating vulnerabilities associated with the current flying armed processes, strengthening covert testing procedures, and improving its processes for reporting security incidents.

### Discussion

TSA appreciates the work OIG has done on its review of issues related to the security of Jackson-Evers International airport, and concurs with many of OIG's recommendations to improve the incident reporting process, travel document checking training, law

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.~~



## Appendix B

### Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

3

enforcement officer flying armed process, and covert test integrity. However, TSA has serious concerns with the Report's analysis and conclusions with respect to covert test integrity and the law enforcement officer flying armed program. As discussed below, TSA disagrees with OIG's conclusions regarding external agency covert testing integrity, and vulnerabilities related to armed law enforcement officers.

#### **TSA Maintains a High Level of Covert Testing Integrity**

##### *Covert Testing Is Not Used to Measure Operational Performance*

As OIG is well aware through its previous work on this topic, covert testing results are only one of many inputs into TSA's security evaluation strategy. Given the nonlinear nature of the risks to transportation security, and our strategy to manage them, TSA relies upon a wide variety of input, including intelligence and workforce feedback, to evaluate and respond to security vulnerabilities.

TSA's Office of Inspection (OI) has a very robust testing program designed to identify systemic vulnerabilities in transportation security systems. Through the OI program, subject matter experts develop and test specific hypotheses regarding potential system vulnerabilities. **These tests are not designed to be performance measures.** Rather, they are evaluations of system vulnerabilities that can be used to design countermeasures. When viewed in this light, the qualitative results from these experiments are highly valuable in analyzing vulnerabilities, with the conclusions from these experiments informing decisions at the strategic level.

Because covert testing provides data at the strategic level, TSA does not rely on covert testing to develop performance metrics. Although Transportation Security Officers (TSOs) receive additional training after a covert test failure, managers' and employees' performance ratings are unaffected by the outcome of a particular test. Rather, covert tests are used to review operational procedures and reinforce training

Considering the role covert testing plays in our security strategy, ensuring the integrity of the covert testing process is of great importance to TSA. As a result, TSA has altered its testing strategy away from red team testing all airports to a strong risk- and intelligence-driven selection process. In addition, we have also altered our covert testing protocols to ensure that advance notice of testing significantly restricted to ensure the safety of covert testers and to obtain unbiased results. As OIG notes in its report, field management officials routinely take steps to ensure the integrity of a covert test, including

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

#### **TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports**

Page 57

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.

## Appendix B

### Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

4

#### *Pervasive Notification of Covert Testing Does Not Exist*

Although OIG agrees that TSA maintains positive test integrity for its internal testing programs, OIG's conclusion with respect to covert testing conducted by outside agencies appears to be the opposite. Based upon its additional investigation into a single incident of an alleged covert test leak, OIG concludes that external covert testing conducted by other federal entities was compromised, and that advanced notification appears pervasive. That conclusion is incorrect and the report offers nothing to support that inflammatory and false accusation. TSA vehemently disagrees with this conclusion and disputes OIG's characterization of the relevant facts.

Any belief that advance notification of covert testing by external agencies is pervasive is sorely misplaced. As OIG should be well aware, TSA has an excellent track record of cooperation with both OIG and the Government Accountability Office (GAO) in relation to covert testing by those organizations. OIG and GAO have tested TSA operations on a regular basis for the last five years without any evidence of a compromise in test integrity created by a TSA employee. There is simply no factual basis to conclude that TSA has ever sought to corrupt covert testing.

In April 2006, OIG conducted covert testing of airport access control systems and challenge procedures in compliance with TSA requirements. These systems are controlled primarily by airport operators and not TSA. **TSA operations were not being tested.** As with all other covert testing, there would have been no benefit to TSA employees to knowingly interfere with any such test, especially when TSA employees were not under evaluation.

As OIG reports, on April 28, 2006, the Acting Assistant General Manager for NETHUB Communications sent a message to TSA field leadership relaying communications taking place between members of the aviation community alerting other members of that community to be on the lookout for a possible compromise of their security. **The alerts circulated within the aviation community for over 24 hours before being received by TSA.** This single message, which was canceled and recalled by the Assistant Administrator for Security Operations 14 minutes after it was sent, forms the sole basis for OIG to conclude that advance notification was "pervasive."

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

#### TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

Page 58

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.

## Appendix B

### Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

5

TSA strongly denies that the transmission of this message, which was later canceled, reflects any intention on TSA's behalf to disrupt covert testing by any outside agency. **This was nothing more than a single incident that was immediately rectified without any evidence of prejudice to OIG's testing.**

Furthermore, if the transmission of this information compromised the testing as has been alleged, **OIG's April 2006 tests were compromised by the airport law enforcement community prior to TSA receiving the message.** As OIG is aware from its investigation, the aviation community was sharing this information among its members for over 24 hours prior to it being received by TSA and shared with TSA personnel. As a result, OIG's assertions that TSA's e-mail revealed key details are not correct. Identical messages had been circulating within the aviation community. The NETHUB e-mail, which is printed by OIG in its entirety, contains no mention of either covert testing or OIG.

Although discounted by OIG, TSA was at the time and continues to be concerned about possible dry-run activities by terrorist organizations. TSA views these activities as attempts to probe or test our security system to observe its responses to potential threats and treats them with as much concern as an actual incident.

OIG's belief that TSA officials should have immediately recognized methods of testing in use by OIG and notified OIG of these messages is also unfounded. The liaison personnel within the Office of Security Operations had limited knowledge of both OIG's testing methodology and the messages circulating in the law enforcement community. In addition, these personnel have additional responsibilities beyond those of liaison with OIG on covert testing. Although we would have preferred to make the connection between the messages and OIG's testing methodology at the time, TSA was concentrating on other operational matters, including the aftermath of a terminal shooting incident in which police officers were severely wounded and one person died at Cleveland Hopkins International Airport.

Accordingly, given TSA's long track record of maintaining positive covert test integrity, and the facts of the incident in question, there is simply no basis for OIG's conclusion that advance notification of outside testing is pervasive.

#### **The Report Overstates Vulnerabilities Related to the Law Enforcement Officer Flying Armed Program**

##### *Vulnerabilities Reported by OIG are Mitigated by Other Program Measures*

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

### TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.



## Appendix B

### Management Comments to the Draft Report

SENSITIVE SECURITY INFORMATION

6

Although the Report addresses serious issues with law enforcement officers flying armed (LEOFA), OIG has inflated the severity of those issues. OIG relies upon a 2006 GAO Report and a 2000 Report from the Bureau of Justice Statistics to state that there are 845,000 Federal, State and local law enforcement officers (LEOs). While TSA has no basis for disputing these figures, their use is misleading – 845,000 LEOs do not fly armed annually. In fact, the breakdown is significantly lower, and nearly the opposite of what the OIG implies.

In its report of September 2005 (“Transportation Security Administration’s Procedures for Law Enforcement Officers Carrying Weapons On Board Commercial Aircraft,” DHS OIG Report # 05-52), OIG published LEOFA statistics more relevant to the issue at hand. The 2005 OIG Report reported 462,000 LEOFA trips annually, far less than this Report implies. Moreover, the breakdown between Federal and State or municipal LEOs described in the 2005 Report was the opposite of what this Report seems to indicate. Approximately 70 percent of these trips were taken by Federal LEOs and only 30 percent by State and local LEOs.

This distinction is very important, as the majority of the vulnerabilities depicted by OIG in this Report concern the verification of the credentialing and letter of authority for state and local LEOs. While TSA does not minimize the risk detailed in this Report and takes seriously any recommendations to improve LEOFA, it appears that OIG’s methodology over-estimates the scope and volume of the State and local LEOFA issue by several orders of magnitude.

Additionally, the Report states that the LEOFA “interim online training system” was not initiated “because of privacy and funding concerns”. This is in fact not the case. After a program review TSA determined that the FBI’s LEO.gov law enforcement portal was the best available vehicle to ensure that the Federal, State and local law enforcement communities had access to the training and the best information possible concerning the program.<sup>1</sup>

#### *Law Enforcement Presence Onboard Aircraft Adds Security Value*

<sup>1</sup> The LEO.gov portal provides cost-effective, time-critical national alerts and information sharing to first responders, law enforcement, and antiterrorism and intelligence agencies in support of the Global War on Terrorism. LEO is provided to members of the law enforcement community at no cost to their respective agencies. It is the mission of LEO to catalyze and enhance collaboration and information exchange across the FBI and mission partners with state-of-the-art commercial off-the-shelf communications services and tools, providing a user-friendly portal and software for communications and information exchange.

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

### TSA’s Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

Page 60

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a “need to know” as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.



## Appendix B Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

7

While some of the Report's recommendations concerning LEOFA are beneficial, a number of assumptions concerning this program and its procedures are flawed. Significantly, the OIG appears to have accepted a number of statements as true, without critically assessing their validity.

For example, the Report states "Senior TSA officials, as well as federal, state and local LEOs describe the flying armed program as the biggest weakness in aviation security." This quote regarding the weakness is wholly inaccurate.

TSA relies upon a system of mutually reinforcing layers of security to protect the traveling public and the Nation's transportation system. There are 19 interlocking layers of security in all -- each capable of disrupting a terrorist attack. Together, their security value is exponentially increased, resulting in a much stronger, formidable system. A terrorist who has to overcome multiple security layers in order to carry out a successful attack is more likely to be pre-empted, deterred, or to fail during the attempt. The system begins with intelligence gathered by the U.S. government that is analyzed, shared, and applied. The system includes checking every passenger manifest against terror watch lists and observing behaviors and activities in the airport environment. The physical screening of passengers and baggage is the most visible element of this system, but behavioral observation, travel document verification and the Visible Intermodal Protection and Response program are included. Finally, the system includes a partnership with airlines, airports, pilots, flight crew members, and the traveling public.

The presence of law enforcement, in airports and onboard aircraft, is an element of the aviation security system. Thousands of Federal Air Marshals (FAMs) are in the air and on the ground, deployed to protect passengers and crew on flights worldwide. In addition, Federal, State, and local LEOs on official travel are permitted to travel armed to provide an additional line of defense and support. The presence of these additional LEOs contributes security value to the protection of this network. Similarly to doctors and emergency medical technicians onboard an aircraft, this measure contributes to passenger safety.

When questioned concerning the merits of this statement, TSA was informed that these statements were made to the OIG by interviewee(s), and as such, they were not the conclusions of the OIG per se. It does not appear from the content of the report, that any effort was made to assess the credibility of the unnamed individual(s) making the assertions, nor was an attempt made to critically examine its merits. Rather, the assertion

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

Page 61

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.~~

## Appendix B Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

8

was accepted as valid on its face, without assessing whether it reflected opinion, overstatement, or a mistake of fact.

### *Planned Program Improvements Will Mitigate Risks*

TSA's Office of Law Enforcement / Federal Air Marshal Service recently chartered a working group to develop improved safeguards for the LEOFA program. The group, which meets monthly with representatives from federal, state, county and municipal police agencies, determined that processes outlined in section of 49 C.F.R. § 1544.219, requiring a state, county or municipal LEOFA to present an original letter of authority from the LEO's employing agency should be improved.

If adopted, the working group's proposed solution will provide a more secure and verifiable alternative to the letter of authority. Under the proposal, State and local law enforcement agencies would establish a LEO's authority to fly armed by sending a secure message to TSA through the National Law Enforcement Telecommunication System (NLETS). NLETS is an international, computer-based message system linking State, local and Federal law enforcement and justice agencies to share information. The mission of NLETS is to provide an international justice telecommunications and information service in a secure environment. Each law enforcement agency is issued a unique Originating Agency Identifier (ORI), a nine-digit code used by agencies on the law enforcement network NLETS.

Under this approach, the message would contain all information in the currently required letter, with the added security feature of validation that the message originates from the parent agency. The requirement for the LEO's employing agency to send a message via NLETS using the unique ORI will add an additional layer of security and diminish current vulnerability posed by potential counterfeit or unauthorized letters. Implementation of this system requires coordination within the law enforcement community, additional resources and a TSA infrastructure to receive, monitor and disseminate notifications to airports.

Federal LEOs are not required to obtain and present a letter of authority from their employing agency. However, in the event that verification is necessary, OLE/FAMS has developed a 24/7 contact list of Federal law enforcement agencies allowing for verification of Federal LEOs seeking entry to the sterile area of an airport.

OIG was briefed on the recommended improvements to the LEOFA process, including use of NLETS messaging, which will evolve into a computer based, independently

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.~~

## Appendix B Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

9

verifiable means of identifying LEOs in the near future. Additionally, OIG was informed about the TSA e-Logbook IT solution which is a secure browser-based application using workstations across a TSA wide network. This program has been successfully piloted; TSA offered a demonstration of this project to the OIG.

Taking all of these factors into account, the assertion that the LEOFA program is the "biggest weakness in aviation security" is substantially overstated.

### *Making LEOFA Requirements Confidential Does Not Add Security Value*

OIG also appears to believe that publication of the LEOFA regulation creates a security vulnerability. OIG states:

Besides TSA and the law enforcement community, other individuals, including commercial airline carrier and other airport authority employees are knowledgeable about the process. Additionally one officer we spoke with expressed concern about how knowledgeable and well versed prisoners are with the flying armed program, given that these prisoners are escorted through this process while in the company of armed LEOs.

TSA does not agree with this assessment. First, OIG appears to advocate that airport operators and air carriers have no need for knowledge of LEOFA procedures or the presence of armed individuals in areas under their control. TSA cannot accept that disregarding or refusing the information needs of our aviation security partners' is a wise practice. Clearly, the success of the LEOFA program depends on maintaining these relationships and partnerships. Second, while OIG is concerned with a prisoner's knowledge of the LEOFA process, it is reasonable to conclude that prisoners may be familiar with certain aspects of the LEOFA program because they are frequently transported on commercial airlines, and may have personally observed the procedures on a number of occasions. Furthermore, the previously noted proposal for secure messaging through NLETS should mitigate the potential for infiltration through the LEOFA program regardless of the availability of the regulation.

The LEOFA regulation provides public notice to Federal, State, local and tribal law enforcement agencies of the legal requirements for an officer to fly armed on a commercial flight in the United States. In addition, it demonstrates to officials and employees of air carriers and airport authorities both that law enforcement officers have specific legal authority to fly armed and that there are standards with which LEOs must comply. To contend that this regulatory construct is a potential harm to aviation security is confusing. In particular, it is difficult to understand how removing or restricting access to this regulation could add security value.

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.



## Appendix B

### Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

10

As was mentioned in earlier correspondence and in meetings with OIG staff, TSA has taken steps to amend the existing Federal regulation concerning LEOFA. TSA offered to brief the OIG regarding the draft proposal last summer. The OIG did not accept this briefing offer though it had the opportunity to do so prior to the publication of its letter report on this topic.

Finally, TSA would note that LEOFA relies on the responsibility and accountability of our airport law enforcement agency partners and those individuals operating under LEOFA authority. A biometric identification system could not prevent an issue like the event OIG is investigating that occurred at Jackson-Evers airport where letters of authority were issued to personnel who did not qualify. The LEOFA program depends upon the honesty of those individuals using it. No future change to the LEOFA regulation, biometric card or enhanced training regimen could ever prevent instances of bad judgment, lack of professionalism or lapses in personal integrity.

#### Comments of a Technical Nature

##### *The LEOFA Process*

The statement of requirements (bullets at the bottom of the page) does not include all the requirements in the regulation. The LEO must be direct employee of government agency, must be sworn and commissioned to enforce criminal or immigration statutes, and must be authorized to have a weapon. The regulation also delineates instances in which an individual would need access to a weapon. Finally, TSA's regulations apply only to regulated parties, not to TSA. TSA's procedures for handling armed LEOs are contained in its Standard Operating Procedures (SOPs).

As part of the boarding procedure, the LEOFA does not inform the pilot, the gate agent is responsible for informing the Pilot In Charge of the presence of a LEOFA onboard. 1544.219(a)(4)(v).

##### *Incident Reporting Process*

TSA Operations Directive OD-400-18-2A "Reporting Security Incidents to TSOC," has been superseded by OD-400-18-2B dated June 22, 2007. The revised OD adds a cargo reporting requirement on page 2. The prior 2A version is also cited at pages 10 and 39.

##### *Position Titles*

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

SENSITIVE SECURITY INFORMATION

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

Page 64

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.

## Appendix B Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

11

Screening Managers are now titled Security Managers. Aviation Security Inspectors are now titled Transportation Security Inspectors.

### *Exit Lanes*

TSA does not control and manage exit lanes at every airport. In general, TSA is responsible solely for exit lanes that are collocated with a security checkpoint. An exit lane may be controlled either through monitoring by personnel or through a one way security barrier such as a door.

### *Enforcement Actions Involving Law Enforcement Officers*

TSA has a direct policy statement with respect to enforcement actions against LEOs. Section 2B-4 of the Office of Security Operations National Inspection Manual (NIM) provides guidance on the process for managing cases involving LEOs. The guidance is as follows:

#### 2B-4. Cases against Law Enforcement Officers

A. General. The Transportation Security Regulations (TSR) explicitly permit LEOs, Federal Air Marshals, and other authorized individuals to carry a weapon at airports and onboard aircraft pursuant to the requirements set forth therein. See 49 C.F.R. §§ 1540.111(b)(2), 1544.219, 1544.221, 1544.223, and 1546.211. In order to carry a weapon, an LEO must have a need to have the weapon accessible and must meet the following specifications:

- 1) Be a Federal law enforcement officer or a full-time municipal, county, or state law enforcement officer who is a direct employee of a government agency;
- 2) Be sworn and commissioned to enforce criminal statutes and immigration statutes;
- 3) Be authorized by the employing agency to have the weapon in connection with assigned duties; and
- 4) Have completed the training program "Law Enforcement Officers Flying Armed."

B. Weapons at the Screening Checkpoint. Civil enforcement action against an LEO should be pursued only where the LEO possesses a

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.

## Appendix B Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

12

prohibited item at a security checkpoint that he or she would not be expected to carry in the ordinary course of his or her duties. Examples include machetes, axes, and throwing stars. Prohibited items that an LEO would be expected to carry in the ordinary course of his or her duties are firearms and batons. Aggravating circumstances may warrant a civil enforcement action regardless of the type of weapon carried by the LEO. Such cases will be especially fact-specific and must be coordinated with Field Counsel.

C. Weapons in Checked Baggage. An LEO must follow the same TSA requirements for firearms and other items in checked baggage that are applicable to all passengers.

D. Contacting the LEO's Employer. Counsel or other appropriate TSA personnel (e.g. AFSD-I or AFSD-LE) may contact an LEO's employer in order to obtain information that may be necessary for the appropriate resolution of the incident. For example, if the status of a person claiming to be an LEO is in doubt because he or she lacks appropriate credentials, TSA may contact the LEO's employer to verify that he or she is, in fact, an LEO. However, if a LEO provides appropriate credentials to demonstrate his or her status as a bona fide LEO, TSA should not contact the LEO's employer unless more information is needed from the employer to further an official TSA investigation.

*WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.*

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

Page 66

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.~~

## Appendix B Management Comments to the Draft Report

---

### SENSITIVE SECURITY INFORMATION

**Transportation Security Administration  
Response to Draft Recommendations  
“Transportation Security Administration Management of Aviation Security  
Activities at Jackson-Evers International and Other Selected Airports”**

**TSA Concurs In Part.** TSA recognizes that verifying state and local LEOFA authority could be improved. Accordingly, it is working with other components within TSA to provide solutions to improve policies and procedures allowing armed LEOs on domestic flights.

TSA's Office of Law Enforcement / Federal Air Marshal Service recently chartered a working group to develop improved safeguards for the LEOFA program. The group, which meets monthly with representatives from federal, state, county and municipal police agencies, determined that processes outlined in section of 49 C.F.R. § 1544.219, requiring a state, county or municipal LEOFA to present an original letter of authority from the LEO's employing agency should be improved.

If adopted, the working group's proposed solution will provide a more secure and verifiable alternative to the letter of authority. Under the proposal, State and local law enforcement agencies would establish a LEO's authority to fly armed by sending a secure message to TSA through the National Law Enforcement Telecommunication System (NLETS). NLETS is an international, computer-based message system linking State, local and Federal law enforcement and justice agencies to share information. The mission of NLETS is to provide an international justice telecommunications and information service in a secure environment. Each law enforcement agency is issued a unique Originating Agency Identifier (ORI), a nine-digit code used by agencies on the law enforcement network NLETS.

Under this approach, the message would contain all information in the currently required letter, with the added security feature of validation that the message originates from the parent agency. The requirement for the LEO's employing agency to send a message via NLETS using the unique ORI will add an additional layer of security and diminish current vulnerability posed by potential counterfeit or unauthorized letters. Implementation of this system requires coordination within the law enforcement

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

**TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports**

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.



## Appendix B Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

2

community, additional resources and a TSA infrastructure to receive, monitor and disseminate notifications to airports.

Federal LEOs are not required to obtain and present a letter of authority from their employing agency. However, in the event that verification is necessary, OLE/FAMS has developed a 24/7 contact list of Federal law enforcement agencies allowing for verification of Federal LEOs seeking entry to the sterile area of an airport.

**Recommendation 2: Implement an action plan that establishes funding requirements, necessary resources, and an implementation timeline for a uniform biometric credential that all law enforcement officers will use to gain access to fly armed on commercial airline carriers. TSA is to report to us biannually on its progress until a uniform biometric credential is operational.**

**TSA Concurs In Part.** TSA has begun developing a plan to meet this recommendation. TSA has initiated a process towards a uniform biometric credential and has implemented an electronic Law Enforcement Officer (LEO) logbook solution (e-Logbook). TSA is defining the law enforcement requirements for each initiative and socializing these initiatives with the law enforcement community.

Any biometric credentialing solution will be based upon existing standards, including Federal Information Processing Standard (FIPS 201-1) biometric based smart cards. Process and technology standards for aviation credentialing that could be leveraged to support the Law Enforcement Officers Flying Armed (LEOFA) program are under development. The fiscal year 2008 and 2009 budgets do not specifically include funding for the development, implementation, and/or maintenance of a LEOFA credentialing requirement.

In the near term, credential verification issues will be resolved through a browser-based e-Logbook. This concept has been developed and initial tests have concluded. The e-Logbook application is available from any properly configured workstation within the certified and accredited TSA network. The process can be utilized to capture the requisite information of all armed LEOs entering the sterile area of an airport using uniform procedures.

The e-Logbook test effort began on March 14, 2008, at Washington-Dulles International Airport (IAD) and expanded to Ronald Reagan Washington National Airport (DCA) on April 3, 2008. These efforts permit program designers to fine tune data entry, data flow, Concept of Operations, and supporting Standard Operating Procedures. In the next

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports



## Appendix B Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

3

phase, TSA will capture “real world” LEOFA data electronically. Once established, the e-Logbook will serve as the platform for later generation biometric based identity verification efforts.

This effort is consistent with the requirements of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53, for a phased approach toward establishing a biometric identity verification requirement. TSA continues to work closely with the Department of Homeland Security and key security partners in this initiative. TSA anticipates these non-biometric based test efforts to evolve into sustainable LEOFA airport procedures within the timeframe stipulated by P.L. 110-53.

Although TSA will endeavor to keep OIG informed of the progress toward a uniform biometric credential, TSA feels the need for biannual reporting is unnecessary. Sufficient information will be available to OIG without the need for additional reporting burdens on TSA.

**TSA Does Not Concur.** This recommendation is operationally unfeasible and will not mitigate the vulnerability cited by OIG. Although it may be theoretically conceivable that an improvised explosive device (IED)

\_\_\_\_\_ would uncover the firearm and ammunition declared during the check-in process. Discovering this firearm would not assist in the credential verification process, and would likely escalate tensions at congested checkpoints.

This recommendation suffers from two distinct drawbacks. First,

\_\_\_\_\_ At least one additional TSO or local LEO would be required to monitor the checkpoint or \_\_\_\_\_. Because such searches would likely not lead to the discovery of IEDs or other harmful items, it is doubtful whether the cost associated with dedicating additional TSA resources or reimbursed LEOs could offset the hypothetical benefit of these searches. Second, \_\_\_\_\_ would identify the LEO as being armed, rather than allowing him or her to proceed more discretely and securely

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA’s Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a “need to know” as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.

## Appendix B Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

4

into the sterile area. This situation would further reduce security if the LEO were escorting a prisoner or dignitary.

Although TSA shares the goal of improving the LEOFA process, it cannot endorse a recommendation that would make LEOs less secure while not appreciably improving the screening detection process. This is particularly true, given the potential benefits that are likely to accrue using the NLETS process described above.

Furthermore, if there is a reasonable belief that an individual seeking sterile area access is not authorized to fly armed, or may be impersonating a LEO, TSA personnel and airport police are required to verify the authority of the individual by agency phone calls, NCIC checks, additional ID checks, and if necessary a complete screening of the individual. Because of this common sense requirement, the measure recommended by the OIG should be unnecessary.

For the security reasons cited above, TSA strongly objects to this recommendation, which would have the unintended consequence of revealing the identity of mission FAMs, thus impeding TSA's compliance with section 4016 of the Intelligence Reform and Terrorism Prevention Act of 2004, which requires TSA to "continue operational initiatives to protect the anonymity" of FAMs. For these reasons, TSA urges the OIG to withdraw or refine this recommendation.

**Recommendation 4:** Ensure that exit lanes are included in the travel document checker operating procedures, and that a second form of government issued photo identification is routinely being reviewed at all exit lanes.

**TSA Concurs:** Revised language to include the "exit lane monitor" in travel document checking procedures has been approved and will be implemented in the next revision of the Screening Management SOP, scheduled for release in the spring of 2008. Checking a second form of government-issued photo ID is a current requirement in the Screening Management SOP.

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.

## Appendix B Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

5

**Recommendation 5:** Develop an enhanced two-level document verification training system for TSA personnel that encompass basic and advanced techniques to identify security features contained in government issued photo identification documents.

**TSA Concurs:** The two-level document verification training system was put in place in early FY08. This training consists of five hours on-line training and three hours of classroom training with scenarios and on the job training.

Training is required for anyone performing Travel Document Checking (TDC). It was developed with the help of the U.S. Customs and Border Protection Fraudulent Document Analysis Unit (FDAU), the Immigration and Customs Enforcement Forensic Document Laboratory, and the United States Secret Service. TSA training instructors (TAIs) were used to train the trainers to rollout this training during the TDC nationwide rollout to all federalized airports from October 2007 to March 2008. TSA recommends that this recommendation be closed.

**Recommendation 6:** Revise covert testing protocols to include testing law enforcement officer commercial airline-ticketing agent check-in and exit lane procedures to gain access to airport sterile areas.

**TSA Concurs:** The Office of Inspection "Access Testing Plan" for the second quarter of fiscal year 2008 will increase access control testing scenarios at airports. New vulnerability testing scenarios designed to introduce IED's into sterile areas, will include false boarding passes, false government issued identification, false Secure Identification Display Area (SIDA) badges and false law enforcement credentials. TSA recommends that this recommendation be closed.

**Recommendation 7:** Revise operating procedures to ensure that Transportation Security Officers and airport police use a standard logbook to record law enforcement officer access to airport sterile areas. Each page of the logbook should be dated and sequentially numbered, and should require TSA employees or airport police officers to initial and record their Secure Identification Display Access number or badge number before allowing a law enforcement officer into the sterile area.

**TSA Concurs:** A standardized Checkpoint Sign-In Log/LEO was implemented TSA wide on March 15, 2008. The Log was developed by TSA's Office of Law Enforcement/Federal Air Marshal Service and contains all of the IG-recommended information. The current form includes the date, officer/agency name, address, and other

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.



## Appendix B Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

6

contact information, credential number information, flight information, names of individuals under escort, and affirmation under penalty of law that the LEOFA training has been successfully completed. A copy of the current logbook form is attached to this response. TSA recommends that this recommendation be closed.

**Recommendation 8:** Petition for a change to the U.S. Code of Federal Regulations, which would require refresher training, on a cyclical basis, for all law enforcement officers flying armed. The change should also require that all law enforcement departments maintain records of such training.

**TSA Concurs.** TSA supports the concept of a LEOFA refresher training element. However, as noted by OIG, training on Federal Air Marshal Service (FAMS) tactical doctrine will likely prove unfeasible due to its sensitivity. Further, such training would necessarily be in-person, for which FAMS lack the necessarily capacity and resources.

As was mentioned in earlier correspondence and in meetings with OIG staff, TSA has completed an initial draft amendment to the existing Federal LEOFA regulation, which includes a requirement for refresher training on regular basis. TSA offered to provide a brief to the DHS/OIG on its progress last summer. The OIG did not accept this offer for such a briefing when it had the opportunity to do so.

**Recommendation 9:** Annually disseminate a letter to all TSA airport security personnel that stresses the importance of the covert testing program and reiterates the penalties for unauthorized disclosures.

**TSA Concurs.** While TSA concurs with the recommendation and will take actions to reinforce the importance of protecting covert test integrity, TSA does not agree with OIG's assertions that an environment of low covert test integrity has been permitted by TSA. Integrity is a core TSA value and cannot be compromised. As Administrator Kip Hawley reiterated in a November 15, 2007, message to the TSA workforce, the honest reporting of events and results is expected of all TSA's employees.

TSA's expectations with respect to the proper handling of information have been clear. The TSA Online Learning Center (OLC) currently includes an online training course on SSI. In addition, TSA annually has an "SSI Awareness Week" at all TSA facilities. In the future, the awareness week will include the purpose of covert testing and the importance to safeguard covert test results.

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.

## Appendix B Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

7

**Recommendation 10:** Require all hub airports to create operation centers, or another centralized reporting procedure, for collecting and reporting the required information for the Freedom Center and Performance and Results Information System for all hub-and-spoke aligned airports.

**TSA Concurs.** TSA issued Operations Directive (OD)-400-30-10, Coordination Center Requirements and Functions, in January 2008. This OD establishes 122 Coordination Centers strategically placed in airports throughout the United States. One of the core functions of the Coordination Center is to streamline and standardize reporting of security incidents to TSA's Freedom Center which is TSA's central point of reporting. 100 of the 122 centers are in operation with the remaining 22 slated to be established by July 1, 2008. TSA recommends that this recommendation be closed.

**Recommendation 11:** Develop a strategy for and conduct outreach to support all Transportation Security Officers knowledge and understanding of incident discovery, reporting, and enforcement processes.

**TSA Concurs.** All Transportation Security Officers (TSOs) are required to complete training developed by the Office of Compliance – PARIS Program and provided through TSA's Online Learning Center (OLC) on incident discovery, reporting and enforcement processes. The specific name of this course is PARIS OLC Incident Reporting Training. TSA recommends this recommendation be closed.

**Recommendation 12:** Develop and deliver training to all Transportation Security Officers on incident report writing.

**TSA Concurs.** Training on incident report writing is included in the PARIS OLC Incident Report Training. TSOs are required to obtain a certificate of successful completion for this course prior to requesting access to the PARIS application. The TSO's supervisor must confirm that the user has been properly trained in how to file reports in the system before granting access. The current statistics show over 2,200 TSOs reporting in PARIS who have completed this training since its inception.

The incident report training identifies processes involved in reporting security incidents and includes the types of information required by Transportation Security Inspectors (TSIs) to conduct a thorough investigation. Applying the training, the TSO is able to identify all pertinent details without requiring an on-scene response by an Inspector.

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.

## Appendix B Management Comments to the Draft Report

---

SENSITIVE SECURITY INFORMATION

8

The training focuses on five key areas of investigative report writing-- who, what, where, when and how -- as well as what information is essential to a PARIS report forming the basis for a possible enforcement action. Emphasis is placed on accuracy and completeness. The training also includes a discussion on the importance of consistency in the narrative report to help all parties engaged in the investigation process to understand, and resolve the matter successfully. The lessons learned from the effective resolution of incidents can minimize and prevent any future ones, thus improving the entire operation.

The learning goals of the training are to enable the user to:

- Understand the purpose of the PARIS Incidents Sub-System;
- Recognize and complete the required fields in the PARIS Incidents System;
- Complete a Paris Incident Report using all the appropriate PARIS Incidents system's functions; and
- Write a well descriptive narrative report to ensure consistent reporting nationwide.

TSA recommends that this recommendation be closed.

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

Page 74

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.



## Appendix C Congressional Request Letter

---

PETER T. KING, NEW YORK  
CHAIRMAN



SENATOR B. THOMPSON, MISSISSIPPI  
RANKING MEMBER

One Hundred Ninth Congress  
U.S. House of Representatives  
Committee on Homeland Security  
Washington, DC 20515

October 6, 2006

The Honorable Richard Skinner  
Inspector General  
Office of the Inspector General  
Department of Homeland Security  
Washington, DC 20528

Dear Inspector General Skinner:

I am writing to respectfully request that you reconsider your October 4<sup>th</sup> decision to decline to investigate the management of aviation security activities at Jackson-Evers International Airport and instead refer the matter to K. David Holmes, the Assistant Administrator for the Office of Investigations at the Transportation Security Administration (TSA). I strongly believe that this decision was a wrong one for the reasons set forth below.

First, my September 11<sup>th</sup> request covered not only the allegations of misconduct by Jackson-Evers International Airport managers but questions about whether TSA personnel can be improperly provided notice as to when a covert testing team is en route. I urged you to take a look at what safeguards are in place to ensure the secrecy of covert testing of aviation security when conducted by your office, the Government Accountability Office, and others. It is important for the integrity of the process that any weaknesses in the covert testing procedures be identified and addressed. To my knowledge, the TSA Office of Investigations' inquiry is not looking into these larger systematic questions. Therefore, you must.

Second, I asked you to look at what protocols and procedures are in place to ensure that when an individual comes to the airport with a firearm or other dangerous prohibited item in their carry-on, TSA headquarters is informed. I wanted you to look at what oversight activities are in place to ensure adherence to these protocols and procedures and whether there are audits of airport records. These questions first arose in relation to the Jackson Airport but I would like a full assessment of the current process and to get some recommendations from you on how the system can be strengthened to ensure that individuals not authorized under Federal law to fly armed cannot do so.

Finally, I believe that an Office of Inspector General inquiry is necessary because there are some concerns as to the manner in which this matter is being examined by TSA's Office of Investigations. Just this week, I wrote to Assistant Secretary Kip

**SENSITIVE SECURITY INFORMATION**

**TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports**

Page 75

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.



## Appendix C

### Congressional Request Letter

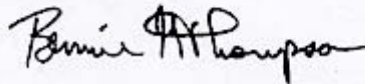
---

October 6, 2006  
Page 2

Hawley to convey the concerns of dozens of Jackson personnel who have personally contacted me. They tell me that only a select few employees, possibly hand-picked by those being investigated, are being interviewed by TSA investigators. I am also concerned that the likelihood of these employees being forthright about problems they observe may be undermined by the location where many of the interviews are being conducted. Jackson staff tell me that the interviews are being done in rooms adjacent to the offices of Mr. Rowlett and his management team—the subjects of the investigation.

For these reasons, I respectfully request that you immediately open an investigation into the matters I have raised. The issues involved are far-reaching and warrant your careful consideration. Please direct any follow up questions you may have concerning this request to Jessica Herrera-Flanigan, Democratic Staff Director and General Counsel of the Committee on Homeland Security, at (202) 226-2616.

Sincerely,



Bennie G. Thompson  
Ranking Member  
Committee on Homeland Security

~~SENSITIVE SECURITY INFORMATION~~

#### TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

Page 76

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.

## Appendix D

### Online Posting of Flying Armed Process

---

**Reference:**

Title 49, Code of Federal Regulations, Section 1544.219

**Definitions:**

**Federal Air Marshals** –specially trained and equipped Federal law enforcement officers assigned to selected flights to take necessary action to prevent hijacking of an aircraft and loss of life. **Protection of their identity is critical.**

**Federal Flight Deck Officer** – a pilot who has volunteered, been selected for, and completed a Transportation Security Administration Training Program, authorizing them to carry a firearm to protect the flight deck of an aircraft.

**Information:**

Full-time municipal, county, and state law enforcement officers are permitted to be armed on commercial aircraft when on official business necessitating a need to have a weapon on a specific flight segment. Some examples of a demonstrated need to be armed are:

- Protective escort duty.
- Hazardous surveillance operations.
- On official business and required to arrive prepared for duty.

An airline has the authority to refuse to allow a law enforcement officer to fly armed.

Sworn personnel are reminded to be discreet in all aspects of flying armed. This includes when notifying the airline representative, presenting the necessary documents, bypassing the Passenger Screening Checkpoint, and while onboard the flight.

After boarding but prior to closing the aircraft's doors, the airline crew must notify the Pilot-In-Command of the airline of each armed law enforcement officer aboard the aircraft. The airline crew must also notify armed law enforcement officers of the location of other armed law enforcement officers aboard the aircraft, including Federal Air Marshals and Federal Flight Deck Officers.

The Pilot-In-Command is the final authority onboard the aircraft.

**Policy:**

Only sworn personnel on official Police Department business who have completed the Transportation Security Administration's Law Enforcement Flying Armed Training Course will fly armed.

Only the Police Chief or an assistant police chief can grant authorization for sworn personnel to fly armed.

## Appendix D

### Online Posting of Flying Armed Process

---

[REDACTED]

Sworn personnel flying armed may not consume alcohol within the eight hours prior to the flight nor consume any alcohol while onboard the flight.

**Procedure:**

- A. Officers Identifying a Need to Fly Armed Shall:
1. Complete Form 17, Authorization to Fly Armed, and forward it through channels for approval.
- B. Airport Check-In Process.
1. Check in at the ticket counter of the affected airline at least one hour prior to flight departure. In emergency circumstances, notify the affected airline as soon as possible if less than one hour.
  2. Identify yourself as a law enforcement officer who is flying armed to the airline representative.
  3. Present the following credentials at the ticket counter:
    - a. [REDACTED] Police Department Identification Card and badge.
      - 1) A badge alone will not be accepted as a means of identification.
    - b. Original Form 17, Authorization to Fly Armed.
      - 1) A photocopy will not be accepted.
      - 2) Retain the original Form 17, Authorization to Fly Armed, for all segments of the flight itinerary.
    - c. [REDACTED] Driver's License.
  4. The airline should issue a "Notice of Law Enforcement Officer (LEO) Flying Armed" form or equivalent.
    - a. Fill out the form completely, accurately, and sign.
  5. If the airline refuses to allow you to fly armed:
    - a. Request assistance from the airline's Customer Service Representative who may be able to assist in resolving issues encountered at the ticket counter or boarding gate.
    - b. If the issue cannot be resolved and the airline still refuses to allow you to board the plane armed, place the unloaded weapon and ammunition in checked baggage.

## Appendix D

### Online Posting of Flying Armed Process

---

- [REDACTED]
- 1) A locked, hard-sided container is required to store the firearm if being placed in checked baggage. Sworn personnel should always bring this item with them in their checked baggage in case the airline refuses to allow them to fly armed.
    - a) Ammunition must be placed in the factory carton or other similar packaging. Ammunition may not stay loaded in the weapon's magazines.

#### C. Check-In Process for Screening Checkpoints.

1. After leaving the airline ticket counter, respond to the checkpoint of the assigned gate.
2. Proceed to the checkpoint exit lane and identify yourself as a law enforcement officer who is flying armed to a TSA agent.
3. Present the following documents for inspection:
  - a. [REDACTED] Police Department Identification Card and badge.
  - b. Original Form 17, Authorization to Fly Armed.
  - c. [REDACTED] Driver's License.
  - d. "Notice of LEO Flying Armed" form.
4. The TSA agent will contact a representative from the local law enforcement agency whose jurisdiction covers the affected airport to respond and verify the credentials.
5. If problems are encountered, request to speak to a TSA Screening Supervisor who may be able to resolve issues encountered at the screening checkpoint.

#### D. Check-In Process at Boarding Gate.



1. Upon arrival at the boarding gate, identify yourself as law enforcement officer who is flying armed to the gate agent and discreetly present the "Notice of LEO Flying Armed".
2. Upon boarding the plane, present the "Notice of LEO Flying Armed" form to the flight crew.
  - a. The flight crew and/or Pilot-In-Command may also request to see your credentials and authorization form.
3. Present the "Notice of LEO Flying Armed" form to the gate agent and flight crew on all segments of the flight itinerary, including transfer and connector flights.



## Appendix D

### Online Posting of Flying Armed Process

---

- 
4. The Pilot-In-Command has the final approval on whether a law enforcement officer will fly armed on the plane.
- a. If the Pilot-In-Command refuses to allow an officer to fly armed, place the firearm in checked baggage.
- E. Officers Flying Armed
1. Shall at all times keep the firearm concealed and out of view of the public, if not in uniform.
2. Shall at all times keep complete control of the firearm on their person.
- a. The firearm may not be carried off the officer's person in any manner, i.e., carried in a purse or placed in an overhead storage compartment.
3. Shall not carry the Department issued chemical irritant or any other type of self defense spray onto a commercial aircraft, even if in uniform.
- a. The issued chemical irritant canister may be carried in checked baggage.
- F. Response to Incidents aboard Aircraft
1. For disorderly passengers and other non-life threatening situations, allow the flight crew to handle the incident. They have been trained to handle most crisis situations.
- a. Only assist if requested by airline personnel.
2. For aircraft hijackings or other life-threatening situations do not take action if there are Federal Air Marshals onboard unless they specifically request assistance.
3. For aircraft hijackings or life threatening situations when there are not Federal Air Marshals aboard, take the necessary action to prevent loss of life or serious physical harm.
- G. Discharging of Firearms aboard Aircraft
1. Officers who are required to discharge their firearm aboard an aircraft to prevent loss of life or serious physical harm are cautioned that shot placement is critical. Errant shots that do not strike an intended target may cause:
- a. Damage to the hydraulic, fuel, electrical systems, or engine of the airplane.
- b. Possible fire.
- c. Serious injury or death to innocent persons.
- 

4

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

Page 80

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.

**Appendix E**  
**Summary of Federal Law Enforcement Officers By Agency**

---

Department of Justice	58,489
Department of Homeland Security*	49,835
Administrative Office of the U.S. Courts	5,528
Department of Treasury	3,766
Department of Interior	3,561
U.S. Postal Service	3,026
Department of Veterans Affairs	2,847
Federal Reserve Board	1,759
U.S. Capitol Police	1,580
Department of State	1,370
Department of Agriculture	813
Department of Labor	795
Smithsonian Institution	787
Department of Health and Human Services	647
Department of Energy	376
Department of Commerce	364
Nat'l Railroad Passenger Corp. (AMTRAK)	331
Social Security Administration	281
National Gallery of Art	278
Environmental Protection Agency	254
Dept. of Housing and Urban Development	227
Tennessee Valley Authority	185
U.S. Supreme Court	139
Library of Congress	114
Department of Transportation	112
Department of Education	97
General Services Administration	56
Nat'l Aeronautics and Space Administration	52
Nuclear Regulatory Commission	46
U.S. Government Printing Office	46
Federal Deposit Insurance Corporation	29
Small Business Administration	27
Office of Personnel Management	24
Agency for International Development	22
Government Accountability Office	16
National Science Foundation	16
Railroad Retirement Board	16
Corp. for National and Community Service	7
Nat'l Archives and Records Administration	4
Peace Corps	4
Equal Employment Opportunity Commission	2
Federal Communications Commission	1
<b>TOTAL</b>	<b>137,929</b>

**Data obtained from GAO-07-121**

\* Department of Homeland Security figures do not include the Federal Air Marshal Service

**TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports**

Appendix F  
TSA Management Comments to OIG-05-52

SENSITIVE SECURITY INFORMATION

1

**TSA Response to DHS OIG Report**  
***“Procedures for Law Enforcement Officers Carrying Weapons  
On Board Commercial Aircraft” (A-04-037).***

**OIG Recommendation 1:** Expedite the selection of the uniform biometric credential to be used, develop and implement a comprehensive plan of action that identifies the work to be completed, milestone completion dates, project cost, and funding.

**TSA concurs.** The Transportation Security Administration (TSA) concurs with the OIG that a uniform biometric credential is needed. Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA) to require TSA to develop a comprehensive law enforcement officer (LEO) credential program and authorized funding; however, no funding was appropriated. Notwithstanding the lack of appropriated funding, TSA has been conducting pilot programs at both Los Angeles International Airport (LAX) and at Ronald Reagan Washington National Airport (DCA) and is in discussions with the Department of Homeland Security (DHS) on leveraging existing infrastructure and resources to meet the IRPTA requirement.

There is a well-recognized need for an identification system for all properly authorized Federal, State, and local LEOs to use in obtaining permission to carry weapons onboard aircraft or access to both the sterile and secured areas of U.S. airports. The topic was the subject of a detailed study conducted by interagency working groups and the Aviation Security Advisory Committee (ASAC). Current regulations require that all LEOs flying armed must be trained, know pre-flight notification procedures, possess an appropriate identification card, and if non-Federal, present written authorization from their agency of the need to fly armed. Additionally TSA requires all Screening Managers, Supervisors and Lead Screeners to take a self-directed, online course on fraudulent credential recognition. More than 11,960 TSA employees have completed this training requirement.

Recent discussions between TSA and the DHS Under Secretary for Border and Transportation Security (BTS) have also focused on this issue. As a result, TSA is working with US-VISIT to identify existing technology and infrastructure to potentially use in the development and implementation of a LEO biometric travel credential. Despite TSA pursuing possible cost-sharing technology, TSA will be responsible for initial start up costs.

In July 2004, TSA began a “registered armed LEO” pilot at Los Angeles International Airport and at Ronald Reagan Washington National Airport as a sub-pilot of the Registered Traveler pilot program. As a result of these ongoing efforts, TSA began to define the template for a law enforcement officer credential that incorporates a uniform biometric identifier technology for Federal, State, and local LEOs. TSA has contacted other Federal agencies that have experience working with both biometrics and smart card credentials to gain additional insight. As a result of its status as a pilot program, TSA has been unable to implement a nationwide program; however, the pilot activities have

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know,” as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA’s Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a “need to know,” as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.~~



## Appendix F

### TSA Management Comments to OIG-05-52

---

SENSITIVE SECURITY INFORMATION

2

recently included a limited expansion of capabilities and are projected to continue through November 2005.

In preparation for future use of a LEO credential verification program, TSA has researched biometric technology and is working on a strategy for installing the technology at over 700 locations throughout the United States. A national rollout of the program could include coordination with personnel from US-VISIT, as well as other TSA programs, such as Transportation Worker Identification Credential and Registered Traveler to develop a workable process utilizing existing capabilities to minimize funding requirements and maximize efficiencies.

In the interim, TSA is expanding current infrastructure and technology to enhance existing security procedures. For example, TSA has completed the online version of the LEO Flying While Armed Course. TSA will begin implementing the course by the end of 2005, providing certificates to non-Federal LEOs who successfully complete the course. This certificate could be reviewed at the checkpoint as an additional verification method.

**TSA non-concurs.** TSA respectfully disagrees with the recommendation [redacted] prior to entering the sterile area. OIG cited two main concerns to support its recommendation to search LEO's carryon luggage. One concern is that an individual could use counterfeit credentials to transport numerous weapons into sterile areas of an airport and onboard commercial flights. A second concern is that [redacted]

allow the LEO to carry hazardous materials (e.g., pepper spray or mace), which are prohibited by Federal regulations implemented by the U.S. Department of Transportation.

TSA has taken steps to mitigate the vulnerability of the potential for fraudulent LEO credentials. A revised TSA LEO Flying Armed Training Program is projected to be available via the internet for State, local, territorial, and tribal LEOs by the end of 2005.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.~~

Appendix F  
TSA Management Comments to OIG-05-52

---

SENSITIVE SECURITY INFORMATION

3

Upon completion of the mandatory training, a LEO will receive a certificate with a unique identifier number. TSA will maintain a record of the unique identifier number and the LEO to whom this number is issued. The unique identifier number can then be verified to assist in situations where there is a question regarding the authenticity of a credential presented by an individual claiming to be a LEO. An additional mitigating measure is the training of screeners and screening supervisors on document identification techniques; this training has already been provided in many airports. TSA will also consider intensifying training for screeners and screening supervisors that further emphasizes identifying elements of document falsification.

There are also operational issues to consider. Most airports are not configured for an [REDACTED] would defeat the purpose of allowing the discreet clearance procedure that prevents other passengers from becoming aware of the LEO's identity and the presence of a weapon onboard the aircraft. Publicly x-raying or physically inspecting a LEO's bag in line at the screening checkpoint or in view of others could cause undue passenger alarm, jeopardize covert missions, and place the flight at greater risk.

**Hazardous Materials.** The OIG also raised a concern about LEOs possibly carrying prohibited hazardous materials onboard a passenger aircraft. [REDACTED]

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

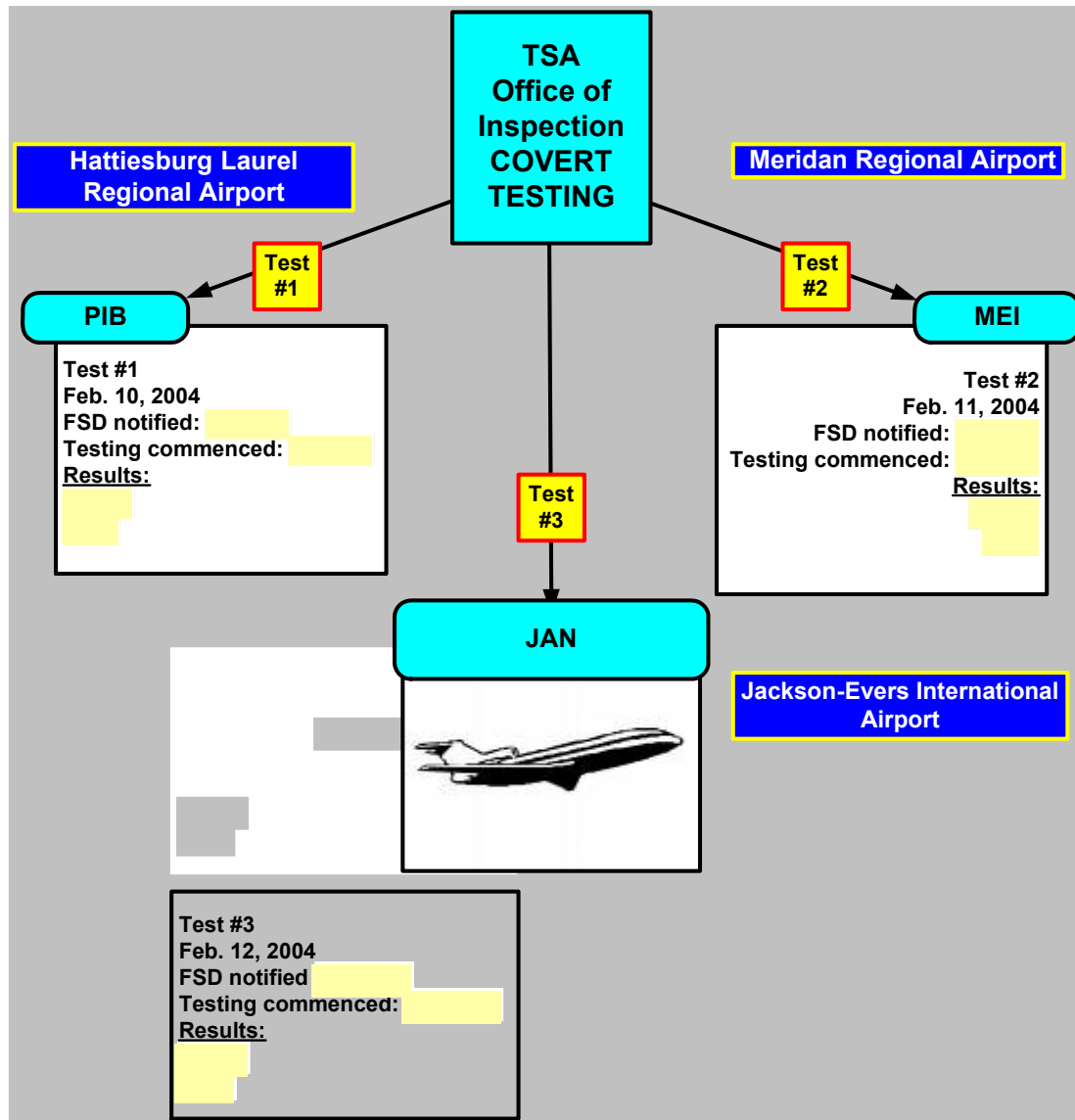
TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports

Page 84

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.

## Appendix G

### Timeline of Covert Testing at Jackson-Evers International Airport



## Appendix H NETHUB Congressional Request Letter

---

BENNIE G. THOMPSON, MISSISSIPPI  
CHAIRMAN



PETER T. KING, NEW YORK  
RANKING MEMBER

**One Hundred Tenth Congress  
U.S. House of Representatives  
Committee on Homeland Security  
Washington, DC 20515**

November 1, 2007

The Honorable Richard L. Skinner  
Inspector General  
Department of Homeland Security  
Washington, DC 20528

Dear Inspector General Skinner:

I write to inform you of some disturbing information that has recently come to my attention concerning covert testing of Transportation Security Administration (TSA) airport screening checkpoints. The attached email, entitled "NOTICE OF POSSIBLE SECURITY TEST," was sent from TSA's "NETHUB" on April 28, 2006 at 2:51 PM to numerous recipients, apparently including all Federal Security Directors and other airport security staff.

The email, which was from TSA's Assistant Administrator for the Office of Security Operations, states that the information is provided for "situational awareness." It goes on to say that airport authorities and airport police received "informal notice" of "possible security testing," and concludes with specific information about the methods the testers are using and a brief description of the testers themselves.

In March of this year, your office issued OIG-07-35, entitled "Audit of Access to Airport Secured Areas." The unclassified summary states that you "performed access control testing at 14 domestic airports of various sizes," and that your "four-person team conducted more than 600 access control tests." Though the unclassified summary of your report does not reveal when and where your testing took place, the email was sent some eleven months before your report. If the email provided advance notice of covert testing during the time period in which your office conducted covert testing, I am concerned that the important oversight work of your office may have been compromised.

Obviously, any effort to undermine the integrity of covert testing of TSA's screening checkpoints is unacceptable. In your August 29, 2007 Letter Report concerning the advance notice of covert testing given to Transportation Security Officers at Jackson-Evers airport in Jackson, MS, you state that you are assessing whether this type of incident was isolated to that airport. I ask that you expand your inquiry to include consideration of all facts surrounding the attached email as well as whether *any* covert testing by any government entity (whether conducted by your office, the Government Accountability Office, or the TSA itself) was compromised by advance warnings.

**SENSITIVE SECURITY INFORMATION**

**TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports**

Page 86

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR part 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR part 1520.

**Appendix H**  
**NETHUB Congressional Request Letter**

---

**November 1, 2007**  
Page 2

Thank you for your assistance with this matter. If you have any questions, please contact Cherri Branson, Chief Oversight Counsel, at (202) 226-2616.

Sincerely,



Bennie G. Thompson  
Chairman

Enclosure

Appendix I  
April 28, 2006, NETHUB Email

---

-----Original Message-----

**From:** NETHUB

**Sent:** Friday, April 28, 2006 2:51 PM

**To:** TSA FSD; TSA DFSD; TSA AFSDS; TSA AFSD-R; TSA AFSD-LE

**Cc:** TSNM COMMERCIAL AIRLINES; TSNM COMMERCIAL AIRPORTS; Schear, James; Morris, Earl R; McGowan, Morris; Restovich, Mike; Tashiro, Susan; NETHUB

**Subject:** NOTICE OF POSSIBLE SECURITY TEST

Date: April 28, 2006

To: Federal Security Directors

From: Mike Restovich, Assistant Administrator, Office of Security Operations

Primary POC: NetHub

Secondary POC: None

Action Due Date: None

Subject: NOTICE OF POSSIBLE SECURITY TEST

This information is provided for your situational awareness. Several airport authorities and airport police departments have recently received informal notice of possible DOT/FAA security testing at airports around the nation. Here is the text of one such notification:

Several airports have reported that the DOT is testing airports throughout the country. Two individuals have been identified as FAA or DOT at the airport in JAX this morning. They have a stack of fake ID's, they try to penetrate security, place IED's on aircraft and test gate staff. These individuals were in CHS earlier this week and using a date altered boarding pass managed to get through the security checkpoint. Alert your security line vendors to be aware of subtle alterations to date info. They should also pay very close attention to the photo id's being presented. They will print a boarding pass from a flight, change the date, get through security (if not noticed) and try to board a flight and place a bag in the overhead. There is a couple, and the woman has an ID with an oriental woman's picture, even though she is Caucasian. We are getting the word out.

Office of Security Operations, NetHub

SENSITIVE SECURITY INFORMATION

TSA's Management of Aviation Security Activities at Jackson-Evers International and Other Selected Airports



## Appendix J

### Major Contributors to this Report

---

Marcia Moxey Hodges, Chief Inspector, Department of Homeland Security,  
Office of Inspector General, Office of Inspections

Angela E. Garvin, Senior Inspector, Department of Homeland Security, Office  
of Inspector General, Office of Inspections

Ryan Carr, Inspector, Department of Homeland Security, Office of Inspector  
General, Office of Inspections

## Appendix K Report Distribution

---

### Department of Homeland Security

Secretary  
Deputy Secretary  
Chief of Staff  
Deputy Chief of Staff  
General Counsel  
Executive Secretary  
Director, GAO/OIG Liaison Office  
Assistant Secretary for Policy  
Assistant Secretary for Transportation Security Administration  
Assistant Secretary for Public Affairs  
Assistant Secretary for Legislative Affairs  
Director of Operations Coordination  
TSA Audit Liaison

### Office of Management and Budget

Chief, Homeland Security Branch  
DHS Program Examiner

### Congress

Congressional Oversight and Appropriations Committees, as appropriate

### **Additional Information and Copies**

**To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at [www.dhs.gov/oig](http://www.dhs.gov/oig).**

### **OIG Hotline**

**To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:**

- **Call our Hotline at 1-800-323-8603;**
- **Fax the complaint directly to us at (202) 254-4292;**
- **Email us at [DHSOIGHOTLINE@dhs.gov](mailto:DHSOIGHOTLINE@dhs.gov); or**
- **Write to us at:**  
**DHS Office of Inspector General/MAIL STOP 2600, Attention:**  
**Office of Investigations – Hotline, 245 Murray Drive, SW, Building**  
**410, Washington, DC 20528**

**The OIG seeks to protect the identity of each writer and caller.**